1986

An investigation of multilevel security and its application in the Wargaming, Research, and Analysis (W.A.R)--lab.

Wall, James A.

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

AN INVESTIGATION OF MULTILEVEL SECURITY AND ITS APPLICATION IN THE WARGAMING, RESEARCH, AND ANALYSIS (W.A.R.) LAB

by

James A. Wall

March 1986

Thesis Advisor: Thomas J. Brown

Approved for public release; distribution is unlimited.

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3 DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution is unlimited.
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4 PERFORMING ORGANIZATION REPORT NUMBER(S)	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION Naval Postgraduate School 6b. OFFICE SYMBOL (If applicable) 74	7a. NAME OF MONITORING ORGANIZATION Naval Postgraduate School
6c. ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000	7b ADDRESS (City, State, and ZIP Code) Monterey, California 93943-5000
8a. NAME OF FUNDING / SPONSORING ORGANIZATION 8b. OFFICE SYMBOL (If applicable)	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State, and ZIP Code)	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT ACCESSION NO

11 TITLE (Include Security Classification)
AN INVESTIGATION OF MULTILEVEL SECURITY AND ITS APPLICATION IN THE WARGAMING, RESEARCH, AND ANALYSIS (W.A.R.) LAB

12 PERSONAL AUTHOR(S)
Wall, James A.

13a TYPE OF REPORT	13b TIME COVERED	14 DATE OF REPORT (Year, Month, Day)	15 PAGE COUNT
Master's Thesis	FROM _____ TO _____	1986 March	93

16 SUPPLEMENTARY NOTATION

17 COSATI CODES			18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
FIELD	GROUP	SUB-GROUP	Multilevel Security, Security Kernel, Risk Assessment

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

This thesis presents a discussion of automated data processing and storage in a multilevel secure environment. The paper covers areas such as the design and implementation of a security Kernel; the DOD Computer Security Center's criteria for trusted computer systems and networks; and risk assessment when processing and storing sensitive or classified data.

One of the primary purposes of this paper is to serve as a handy reference for students in the Command, Control, and Communications curriculum at the Naval Postgraduate School who will research multilevel security and secure guard applications following the acquisition of the Gemini Trusted Multiple Microcomputer Base for the Wargaming, Research,

20 DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION Unclassified
22a NAME OF RESPONSIBLE INDIVIDUAL Thomas J. Brown	22b TELEPHONE (Include Area Code) 408-646-2772 22c OFFICE SYMBOL 62Bb

DD FORM 1473, 84 MAR 83 APR edition may be used until exhausted
All other editions are obsolete

SECURITY CLASSIFICATION OF THIS PAGE

19. and Analysis (W.A.R.) lab.

Additionally, a risk assessment of the W.A.R. lab was conducted and the possibilities of converting the facility into a multilevel secure computing environment were investigated.

Approved for public release; distribution is unlimited

An Investigation of Multilevel Security and Its Application in the Wargaming, Research, and Analysis (W.A.R.) Lab

by

James A. Wall
Captain, United States Army
B.S., North Carolina State University, 1977

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN SYSTEMS TECHNOLOGY
(Command, Control and Communications)

from the

NAVAL POSTGRADUATE SCHOOL
March 1986

ABSTRACT

This thesis presents a discussion of automated data processing and storage in a multilevel secure environment. The paper covers areas such as the design and implementation of a security kernel; the DoD Computer Security Center's criteria for trusted computer systems and networks; and risk assessment when processsing and storing sensitive or classified data.

One of the primary purposes of this paper is to serve as a handy reference for students in the Command, Control, and Communications curriculum at the Naval Postgraduate School who will research multilevel security and secure guard applications following the acquisition of the Gemini Trusted Multiple Microcomputer Base for the Wargaming, Research, and Analysis (W.A.R.) lab.

Additionally, a risk assessment of the W.A.R. lab was conducted and the possibilities of converting the facility into a multilevel secure computing environment were investigated.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

I. INTRODUCTION

The rapid expansion of information systems and networks in the command and control world have made them a critical link in the national defense. "Computers' . . . speed and unfailing accuracy make them well suited to the massive information handling tasks in battle management for: shared information storage, retrieval, and dissemination systems; rapid and common data processing systems; and efficient and reliable communications process control." [Ref. 1:p. 271] Unfortunately, the rapid pace of technological breakthrough in computing systems has far outpaced developments in computer security. Abuses of computers that were not designed from the ground up to provide security currently represent a major problem. For these systems, a great need exists for a front-end processor to authenticate and control access to the system or its resources.

A. HISTORICAL PERSPECTIVE

In the mid-1950's to the early 1960's, data processing was usually confined to a single center. Programs were brought to the computer center in the form of card decks. These programs were batch processed and any sensitive or classified data could be purged prior to the next user. Since there was no sharing of resources, physical security of the sensitive or classified data and assurance of a cleared memory were the major components of any security policy.

As more powerful and faster computers emerged in the mid-1960's, "operating-systems" evolved to allow multiple users. This was a result of the computers' cost and the fact that human operators were too slow to efficiently employ the machines. Simple operating systems selected which jobs would run on a priority basis. More dynamic operating systems allowed several jobs to run at the same time by the use of "multiprogramming". Even more sophisticated yet were operating systems that allowed "time-sharing". Many users were allowed access to the computer through remote terminals. Although all of these users were being serviced at the same time, each user had the illusion of being connected to a dedicated computer. The computer was now under the control of a computer operating system rather. than the user. These privileged operating systems soon became the target of malicious users who wanted to penetrate the operating system and share their privileges. Suddenly, computer security became an issue. The need for "trustworthy" operating systems was apparent.

B. COMPUTER SECURITY

"Computer security is the protection of computing assets or resources and computer-based systems against accidental and deliberate threats whose occurrence may cause losses due to those systems' non-availability, lack of integrity, or lack of confidentiality." [Ref. 2:p. 7]

1. Physical Security

This is the most basic security requirement and should be afforded to all computer systems with considerations given to both the internal and external environments. The degree to which physical

security is insured is dependent upon the value of the data being protected. Essentially, most of the considerations given to the physical security of computers is not unique to computers and is closely related to the security given classified documents.

2. Security Modes of Operation

Information can also be protected from compromise by the particular security mode of operation that is selected. The Department of Defense recognizes five distinct security modes of operation. These modes are enumerated in Appendix A. Security modes of operation fall into one of two general categories: dedicated usage or shared resources.

In the dedicated mode, access to the computer system is restricted to an individual user or homogeneous group of users that have access to all the information that is processed or stored on the system. There is no danger that subversion or failure of the computer will result in the compromise of sensitive information. The computer security problem in this category is one of physical security and personnel screening.

Resources are most often shared among groups of users with a common level of trust to add some flexibility to the dedicated mode. Again, physical security and personnel screening are paramount to such a security policy and all resources/terminals tied to the system must be afforded the same degree of protection. Today's problem is one of being able to share computer resources among users or groups of users that do not share the same level of trust (multilevel security).

3. Communications Security

Remote and interactive access to computers give rise to a new threat to information security. Information that is being transmitted through any medium is susceptible to interception. The most common means to combat this threat is data encryption. This technique involves the use of encryption algorithms usually seeded by some variable key to produce unintelligible code prior to transmission. This code can then be deciphered upon receipt.

Although not strictly a communications security problem, emanations security (TEMPEST threat) is mentioned at this point because the same principles of sending and receiving electromagnetic signals are involved. Emanations are electromagnetic energy by-products of computing devices that are usually most severe when communicating with peripherals. These emanations can be detected by sensitive devices for several hundred yards. Cathode ray tubes (CRT's) are especially noted for their signatures. Protection, such as shielding, is technically simple but often awkward and expensive and operationally complex.

4. Authentication

Authentication systems have been in use for a relatively long time. They are absolutely essential as an access controller in an environment of shared resources. The most commonly used is that of the password. "The password serves essentially as a "combination" to a "lock" allowing access to the system." [Ref. 1:p. 274] This type of approach is particularly vulnerable when simple passwords are used, compromise of the password is allowed, or a computerized password generator is used to determine the password (especially if the system

does not time out after a number of attempts). Finally, this type of access control permits or prevents access to the computer system, but it fails to distinguish between the various authorized users. This function is dependent upon the internal controls of the computer itself.

This technical weakness can be overcome by the development of a well-formulated security policy that is conveyed to the system designers. The system can then enforce access control mechanisms based on the authorizations it has been given. A trusted system is the result when this process has been successfully accomplished and a well-defined policy regarding access to sensitive information is enforced by the system.

The main requirement for a security policy that is to be integrated into a trusted system is the need for security "labels" for all information to indicate its sensitivity and for all users to indicate their authorization for access. Recent research has shown that an effective labelling policy can be implemented with a two-part label. "The first part represents a hierarchical sensitivity level, such as confidential, secret or top secret; the second, user community of interest or compartment label." [Ref. 1:p. 275]

An operating system must maintain these labels internally so that it can enforce the security policy. The technology is currently available, along with mathematical models and formal specifications, to accomplish this task. The most predominant approach is that of the security kernel (to be explained later). Honeywell Information Systems, Inc. and Gemini Computers, Inc. are on the cutting edge of this technology and are among the few vendors actively marketing such trusted

systems. This paper concentrates on these trusted systems and their use as a multilevel security system and/or a secure guard.

C. DEVELOPMENT OF MULTILEVEL SECURE SYSTEMS

The need for systems that can provide a multilevel secure environment have been well established as a result of the advent of distributed computing systems and shared resources. Alternatives (benign environment or "system-high" concept) to such systems are unacceptable for many Department of Defense applications. The alternatives to a multilevel secure system are defined in DoD Directive 2500.28:

a. clearing all users to the highest level of information on the system and processing all work at that level, or

b. processing jobs of different levels at different times - requiring a complete system change or sanitization each time the level is changed.

A system operating in either of these unilevel modes is usually operating "system high." Either of these choices is inefficient and costly.

In 1968-1974, "Tiger Teams" were formed to attempt penetration of access control mechanisms of existing operating systems. Remarkably, penetration was accomplished on every commercial operating system. The research community became so concerned that public awareness was heightened and such issues were the impetus for the development of the security kernel which provides the basis for multilevel security.

In 1972, the Air Force Electronic Systems Division (ESD) conducted an in-depth analysis of the requirements for a security system. The basic concept of a reference monitor or a security kernel was the

result. This concept was the foundation for work at the Massachusetts Institute of Technology, the MITRE Corporation, and Honeywell Information System to begin restructuring the MULTICS operating system.

In 1977, the Department of Defense initiated an effort to produce the DoD Kernelized Secure Operating System (KSOS) which would emulate the UNIX operating system. The UNIX operating system was chosen because of this operating system's use on the popular PDP-11 series of computers. The implementation phase was contracted out to the Ford Aerospace and Communications Corporation in May, 1978. This project became known as KSOS-11 and further development of the operating system was oriented towards the DEC PDP-11/70.

In a joint effort with the Air Force, Honeywell Information Systems began developing KSOS-6 in October, 1977. This effort was a continuation of the restructuring of the MULTICS operating system. Research was stop and go based on budgetary and other limitations. However, a standard commercial product called the Secure Communications Processor (SCOMP) was the final result. The system is based upon Honeywell's DPS 6 16-bit minicomputer and the MULTICS operating system. SCOMP has been verified by the DoD Computer Security Center as having an A1 level of security. A discussion of the DoD Computer Security Center's criteria for the various levels of security will be presented in Chapter 3.

One of the latest systems to be fielded is the Gemini Trusted Multiple Microcomputer Base by Gemini Computers, Inc. A microcomputer was chosen as the base because it holds great promise serving as a front-end processor because of its physical separation and its small

operating system. In the role as a front-end processor for communications, it can easily handle encryption, decryption, and sending and receiving. This system is currently being evaluated for a B3 level of security and will be discussed later in this paper.

Much research on multilevel secure and guard systems was done concurrently with the above efforts and much has been done since. For a more complete look at these and other efforts, refer to Appendix C [Ref. 3: pp. 90-93]. This information is current as of July 1983.

D. OBJECTIVES

The primary objective of this paper is to serve as a reference on the concept of multilevel security for students in the Command, Control, and Communications curriculum at the Naval Postgraduate School who will conduct research on the Gemini Trusted Multiple Microcomputer Base that is scheduled to be purchased for the W.A.R. lab during the current fiscal year. Additionally, an investigation will be conducted to determine the utility of this system (other than research) in the lab.

Since the reference monitor concept (and specifically the security kernel) is the most widely accepted model for multilevel systems, a discussion of the design and implementation of such models will be presented. This discussion details the requirements for the security kernel and presents various verification techniques.

The combination of hardware and software for the purpose of enforcing a security policy is the basis for the trusted computer system or network. The criteria established by the Department of Defense Computer Security Center for evaluating these trusted systems is examined in detail since they have tremendous impact on all computer

systems and networks in the Department of Defense that process or store sensitive information.

Much of the information concerning trusted computer systems and networks is necessary for the understanding of the discussion of risk assessment. Risk assessment is an attempt to evaluate the level of risk inherent to a system based upon the computing environment. Two methods of risk assessment will be compared and contrasted. Risk assessment usually involves determining the security level of the user and the sensitivity of the information that is being stored or processed on a system. Throughout this paper the term "security level" will be used to denote the combination of clearance (or classification) and formal compartment (or category set). Appendix B lists the security clearances currently recognized by the DoD Computer Security Center.

Finally, a risk assessment of the Wargaming, Research, and Analysis (W.A.R.) Lab will be presented. These findings will help support an investigation of the integration of the Gemini Trusted Multiple Microcomputer Base into the W.A.R. lab .

II. SECURITY KERNEL DESIGN AND IMPLEMENTATION

A review of design and implementation guidelines for the security kernel is relevant for any discussion of multilevel security. Most experts agree that, at the present time, the security kernel concept (introduced by Roger R. Schell in 1972) is the most viable approach to meeting security requirements wherever the need exists for a system that processes shared information. In 1974, MITRE successfully tested a security kernel consisting of only twenty primitive subroutines to manage physical resources and enforce protection constraints to prove that this concept was valid.

A. THE REFERENCE MONITOR CONCEPT

The security kernel approach is based on the reference monitor concept adapted from the models of Butler Lampson (Figure 2.1) [Ref. 4: p. 15]. "A reference monitor is a computer system component that checks each reference by a subject (user or program) to an object (file, device, user, or program) and determines whether the access is valid under the system's security policy. To be effective, such a mechanism must be invoked on every reference, must be small enough so that its correctness can be assured, and must be tamperproof." [Ref. 3:p. 88]

The security kernel can best be described as the hardware and software that transforms the abstract concept of a reference monitor into the reality of a functional security system (Figure 2.2) [Ref. 4: p. 17]. During the design and implementation of the security kernel,

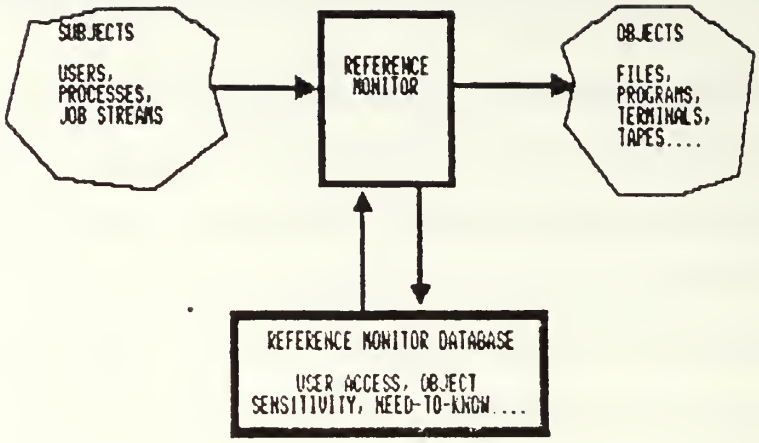

Figure 2.1 - Reference Monitor

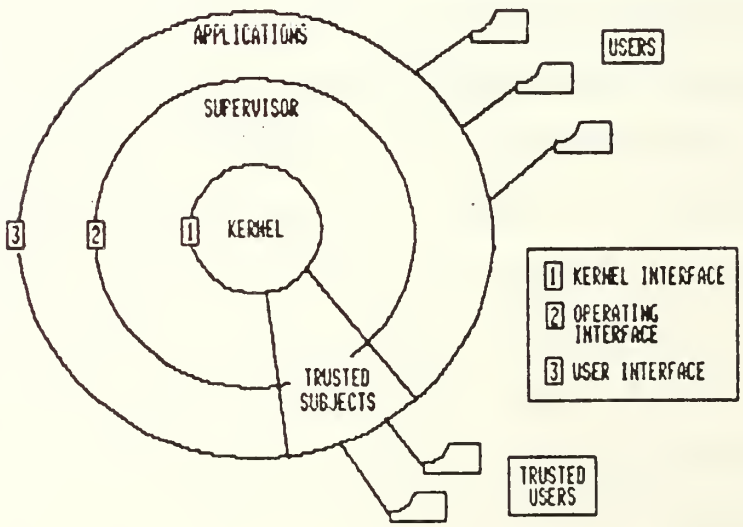

Figure 2.2 - Structure of a Kernel-Based Operating System

total adherence to the following three engineering principles must be observed - completeness, isolation, and verifiability. Every access to system information must be mediated by the kernel (**completeness**). The kernel must also be sufficiently protected to prevent tampering (**isolation**). Finally, there must be a close correlation between the formal security policy and the effectiveness of the security kernel (**verifiability**). The completeness and isolation requirements are best met with hardware foundations and verifiability strengthened by a formal development methodology [Ref. 4:p. 15].

When the need for a "secure" system arises, a list of demands that would insure the desired level of security must be established. Once this has been accomplished, these demands provide the basis for the establishment of a formal security policy. All the permissible modes of access between all subjects and objects must be addressed. These steps must precede the development of a kernel-based system and this formal policy is a primary distinction between the security kernel-based system and other efforts to develop security-relevant operating systems. Concisely, the development of the security kernel-based system encompasses both policy and mechanism.

The security policy is best described by a set of mathematical relationships which provide the basis for a formal security model. In order to be sufficient, the model must define the overall protection behavior of the system as a whole and present a "security theorem" to insure that the behavior of the model always complies with the security requirements of the applicable policy [Ref. 4:p. 15]. The policy must also address both discretionary access rules (applicable to all users)

and nondiscretionary access rules (optional rules applicable to certain users).

1. The Bell and LaPadula Model

The model most widely used for security kernel development is referred to as the Bell and LaPadula model which is the product of early security kernel work at MITRE and Case Western Reserve University. This model represents the kernel as a finite state machine and defines rules for allowable transitions from one secure state to another. Within the model, an access class (a security identifier) is assigned to each subject and object of the reference monitor. Allowable access to objects is made by comparing the access class of both subjects and objects at each transition state. The access classes are organized in a mathematical structure called a lattice or protection matrix. The lattice arrangement defines relationships among the access classes to determine if one access class is greater than, less than, equal to, or not comparable to another class.

Figure 2.3 [Ref. 5:p. 212] shows a hypothetical representation of a protection matrix access diagram located within a security kernel. In this example, User B is considered to be the system administrator. It is clear that his privileges far exceed those of User A. Also, this representation shows that other programs or functions, such as the Editor Command Module, are allowed to operate within established limits. Such an access matrix must reside in the security kernel to insure its integrity.

The model contains two fundamental nondiscretionary rules - simple security condition and *-property. The simple security condition

OBJECTS / SUBJECTS	TIME SHARING SUB-SYSTEM	EDITOR	FILE A1	FILE B1
USER A	ENTER	ENTER	CREATE DELETE READ WRITE EXECUTE	EXECUTE
USER B	ENTER MODIFY	ENTER	READ WRITE EXECUTE	CREATE DELETE READ WRITE EXECUTE
EDITOR COMMAND MODULE	ENTER	READ		

Figure 2.3 - Protection Matrix Access Diagram

allows a subject at a given security level to have read access only to objects at the same or lower security levels (no read up). Simply stated, this rule prevents unauthorized personnel from directly viewing information for which they do not have proper access. The *-property prevents a subject from having write access to objects at lower security levels (no write down). This rule was established to combat "Trojan horse" software and prevents users from unauthorized indirect viewing of information.

The model also includes rules to protect the integrity of the system's information and to prevent improper alteration. Subjects of one access class cannot alter objects located in a higher class. Conversely, a subject of one access class cannot be altered by objects of a lower access class.

Provisions also exist in the model for discretionary access. Authorized users and programs can arbitrarily grant and revoke access to information based on user names or other information.

One limitation of the Bell and LaPadula model, as with most other models, is the lack of safeguards against denial of service. Denial of service is the threat of intentional or unintentional disruption or degradation of service. However, the inclusion of a security kernel does not affect the system's susceptibility to the threat of denial of service. This shortcoming is attributable to the difficulty of establishing a mathematical model to represent the rules.

B. THE DEVELOPMENT PROCESS

Once a security policy has been formalized and an appropriate model has been selected, the development process must be divided into small

increments for implementation. "One common technique is to apply a hierarchy of abstract specifications to the design of the security kernel. For each step, it is important to demonstrate security so that we have confidence in the security of the final system." [Ref. 4:p. 16] Figure 2.4 is a depiction of the integration of the model, the hierarchy of specifications, and the high-level language implementation [Ref. 4: p. 17].

Three classes of formal verification techniques during the kernel development process are also shown in Figure 2.4. The first class is used to prove that the kernel responds as outlined in the formal high-level interface specification. Security flow analysis is often used to analyze information flow in a specification. The second class of verification tests the correctness of mappings between intermediate specifications in the hierarchy and interface specifications. The third and most traditional technique is the verification of implementation to specification.

The kernel provides a relatively small subset of the operating system's functions. The kernel primitives that provide the interface of this subset to the remainder of the operating system are often referred to as the supervisor. General-purpose operating system functions used by the applications are provided by the supervisor primitives.

Functional areas such as process management, file system management for segments, and I/O control comprise the operating system. Each of these areas possibly have security relevant functions that must be in the security kernel. The policy model should identify these security relevant functions. Of particular importance is the kernel's role in

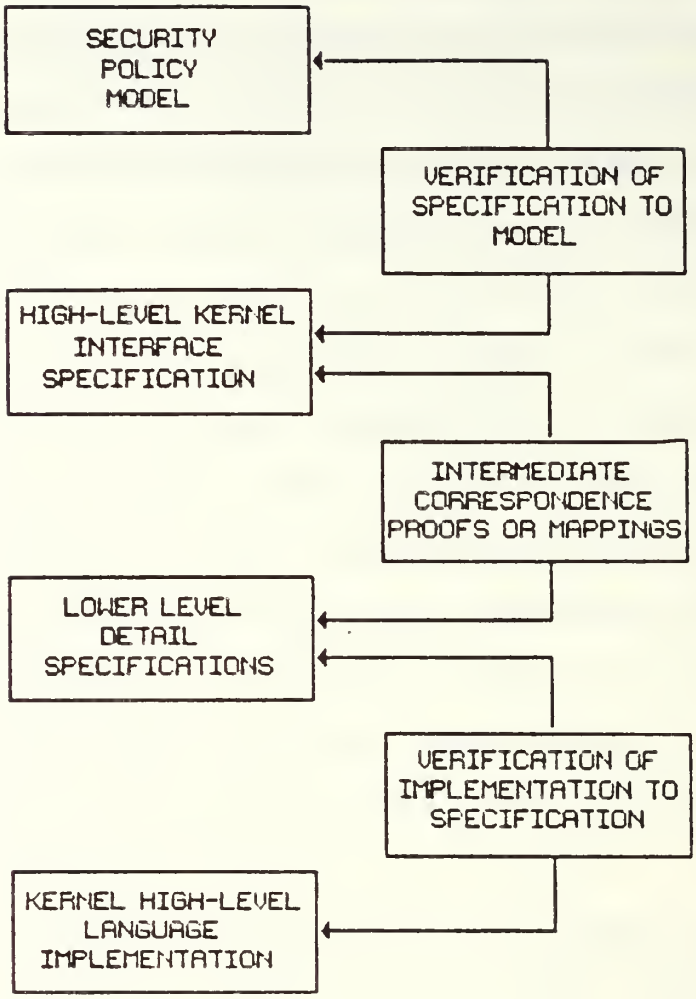

Figure 2.4 - Development and Verification Hierarchy

managing system resources such as memory and disk space that are shared by multiple users. These functions are located in the kernel because they must be virtual (realized by the combination of hardware and software) in order to hide their location from untrusted software. It is permissible for any utility controlling anything not shared by users to be located outside the kernel (in the supervisor).

The basic security model that has been described thus far is rudimentary and most likely the greatest need exists for a system that can be tailored to meet specific requirements that may change from time to time. A kernel that is written so that it is adaptable usually has a group of interfaces that can be invoked by individuals/programs with special privileges - trusted subjects. Internal identifiers such as privilege indicators allow actions such as certain system maintenance activities and access control for nontrusted subjects (Figure 2.2) [Ref. 4:p. 17]. Trusted subjects utilize trusted processes and trusted functions to perform such routine tasks as maintenance of the system's access roster and the upgrading or downgrading of classified material when appropriate.

1. Security Kernel Design and Implementation

The design of the security kernel can approach two extremes when considering the degree to which the kernel implementation is to be founded in hardware. At one extreme, the kernel is entirely written in software and can be run on any conventional machine. In this case, the kernel interprets every user instruction and disallows direct user instructions to hardware. The only hardware involvement is its execution of the kernel software. The other extreme is the total

implementation of the Kernel as hardware instructions which places absolute responsibility for security on system architecture. Obviously, tradeoffs must be made between hardware and software with respect to complexity, size, and performance.

Specific hardware and software mechanisms from four general architectural areas have contributed to varying degrees to supporting a Kernel-based general-purpose operating system. These four architectural areas are: explicit processes, memory protection, execution domains, and I/O mediation [Ref. 4:p. 18].

Explicit processes refer to the need for support for multiple processes (multiprogramming) and interprocess communications. Access decisions for subjects are made on the basis of the user's identification and access class. These two identifiers must be impossible to counterfeit and are tied to each process. In an on-line system, multiple users must be serviced, thus the Kernel must support multiple simultaneous processes. This creates the need for a greater number of process switches and makes efficient process-switching mechanisms such as high speed memory more desirable.

Memory protection requires large segmented virtual memory, access control to memory, and explicitly identified objects. Memory is the usual realization of the reference monitor concept of storage object. Virtual memory and the use of some form of descriptor are commonly used together to serve as an interpretive mechanism to mediate all access to memory.

All information within the system must be represented by distinct, identifiable objects. The virtual address space of an object

includes more than one object. Each has its own distinct logical attributes such as size, access mode, and access class. This logically distinct memory is called a segment.

Virtual memory segmentation is usually supported by hardware. The mapping for segments to virtual address is controlled by a descriptor. This descriptor has not only logical attributes but contains both a physical base address and a segment size which uniquely identifies each segment. The segment descriptor must support the access modes of at least null, read, and read-write for each segment in order to provide adequate discretionary and nondiscretionary access policies. These segment descriptors are managed by the security kernel software. However, the address-mapping hardware still plays a significant role in the actual access mediation process.

Although access to segments is dependent upon unique descriptors, the possibility of an unintentional leakage of information by use of control information such as file names and attributes and system variables maintained within the kernel database still exists. Strict design and verification techniques can prevent or detect this deficiency. The discovery of such a leakage channel late in the kernel's development is a formidable problem for the kernel designer.

Execution domains are necessary for the isolation and protection of the security kernel mechanism. In order for security kernel functions to be invoked, the total address space of the process must include the programs and data of the security kernel. When the process must access segment descriptors, it is necessary for this execution to take place in the kernel only. This requires a separate

execution domain for the security kernel. It is also desirable to keep the supervisor separated from the applications software. A domain structure with three hierarchical domains (kernel, supervisor, and user) is necessary to keep the user and the operating system separated.

Efficient transfer of control between domains is a desirable feature because of the vast number of calls a process makes to the kernel and the supervisor. Access to the most privileged domains of the system must be characterized by a few, carefully defined entry points or security will reduce speed dramatically.

Input/Output mediation can best be handled by a hardware architecture (e.g., I/O processor) that allows direct user or supervisor domain access to I/O. This requires the use of a descriptor to control access to devices similar to the descriptors used for access to memory.

2. Verification

The final comment about security kernel design and implementation concerns verification. Verification technology has not fully matured and is limiting. At the present time, the greatest degree of success has been associated with specification verification such as the flow analysis method mentioned earlier in Section B of this chapter.

III. DOD TRUSTED COMPUTER SYSTEMS AND NETWORKS

Two publications having possibly the greatest impact on multilevel security in computers and distributed systems of computers or networks are products of the Department of Defense Computer Center located at Fort Meade, Maryland. They are the Department of Defense Trusted Computer System Evaluation Criteria (CSC-STD-001-83) dated 15 August 1983 and the Department of Defense Trusted Network Evaluation Criteria (currently in Draft) dated 29 July 1985. These two publications will be discussed in some detail since the blueprint for all acceptable systems must conform to these criteria and the current vernacular of trusted systems can be traced to these documents.

A. TRUSTED COMPUTER SYSTEMS

The publication, Department of Defense Trusted Computer System Evaluation Criteria was written by the Department of Defense Computer Security Center in accordance with DoD Directive 5215.1, "Computer Security Evaluation Center." The purpose of document is to establish a "uniform set of basic requirements and evaluation classes for assessing the effectiveness of security controls built into Automatic Data Processing (ADP) systems." [Ref. 6: p. i] Any ADP system used for the processing and/or storage and retrieval of sensitive or classified information by the Department of Defense is to be evaluated using the criteria defined in the document. This publication is commonly referred to as the "orange book."

Many of the criteria presented in this publication originated from work done by the MITRE Corporation and the National Bureau of Standards (NBS) prior to the formation of the DoD Computer Security Center in January 1981. These standards fulfill two distinct sets of requirements: 1) specific security feature requirements; and 2) assurance requirements. The specific security features are primarily oriented towards information systems employing general-purpose operating systems rather than applications programs being supported. The assurance requirements are applicable for all computing environments ranging from dedicated controllers to full range multilevel secure resource sharing systems [Ref. 6: p.2].

1. Fundamental Requirements

A secure computer system must limit access to information and allow properly authorized individuals or their appointed represenatives only to read, write, create, or delete information. Six fundamental requirements are presented as absolute essentials in obtaining such a secure system. Four of these requirements deal with the actual needs to be provided to control access to information and two deal with assurances that this access to information is in fact being controlled and that a trusted computer system exists.

The first two requirements involve an organization's policy towards computer security:

Requirement 1 - Security Policy

The system must be capable of enforcing an explicit and well-defined security policy to insure that only personnel with proper access (to include discretionary access) are allowed access to the system. Security policy design should be influenced by the perceived threats, risks and goals of the organization.

There are two types of security policy to be considered: mandatory security policy and discretionary security policy. Mandatory security policy establishes a set of rules that permits or denies access to material based directly on the individual's clearance or authorization. Discretionary security policy takes the permission or denial of access one step further and is the principal type of access control available in computer systems today. Not only must an individual be authorized access to information, but a need-to-know requirement must also exist. It is important to note that a discretionary policy is to be developed in addition to the mandatory policy and not as a substitute.

Requirement 2 - Marking

Objects must be marked with access control labels that conform to the mandatory security policy. These labels must identify the sensitivity or classification of the object and the mode of access for authorized users. Whether used internally or as output, accuracy and integrity of the security labels is paramount.

The third and fourth requirements are concerned with accountability:

Requirement 3 - Identification

The computer system must be able to mediate access to information by identifying authorized users and determining their level of clearance and their need-to-know. Once identification of the user has been established, there must be a means of authentication.

Requirement 4 - Accountability

Audit information must be recorded so that all transactions affecting system security can be traced to the responsible party. This information log must be protected from any tampering that would alter or delete such an audit trail.

The final two requirements involve assurance that the computer system is secure:

Requirement 5 - Assurance

The computer system must contain hardware/software mechanisms that can be individually evaluated to assure adherence to Requirements 1-4. Two types of assurance are needed: life-cycle assurance and operational assurance.

"Life-cycle assurance refers to steps taken by an organization to insure that the system is designed, developed, and maintained using formalized and rigorous controls and standards...Operational assurance focuses on features and system architecture used to insure that the security policy is uncircumventably enforced during system operation." [Ref. 6:p. 60]

Requirement 6 - Continuous Protection

The computer system must continuously provide the protection outlined in these fundamental requirements before it can be judged a trusted system.

2. The Criteria

The criteria set forth by this publication are divided into four hierarchical divisions: A: Verified Protection, B: Mandatory Protection, C: Discretionary Protection, and D: Minimal Protection [Ref. 6:p. 5]. They are arranged from the highest level of security to the lowest level respectively. The step up from one Division to another represents a significant increase in security. Divisions B and C are further subdivided into classes that are arranged in a hierarchical manner based on the security mechanism that they possess. A rating for a particular system is based on thorough testing of the security- relevant portions of that system. The security-relevant portion of the system is spoken of collectively as the Trusted Computing Base (TCB). Each class is described by four major sets of criteria: Security Policy, Accountability, Assurance, and Documentation.

Division D: Minimal Protection has only one class and is reserved for systems that have been evaluated, but failed to achieve the standards of a higher class.

Division C: Discretionary Protection contains two classes that provide discretionary access to information and the means to audit and account for such usage. The two classes are: Class C1: Discretionary Security Protection and Class C2: Controlled Access Protection.

The Trusted Computing Base (TCB) of Class C1 satisfies discretionary access requirements by separating users and data. The

Class C1 environment is expected to be one of cooperating users processing data at the same level of sensitivity [Ref. 6:p. 12]. Identification and authentication are required to determine authorized individual or group users.

The discretionary control of Class C2 is made more positive through login procedures, auditing of security-relevant events, and resource isolation. The emphasis is on the individual user in this class. By limiting usage to individuals or groups of named individuals accountability for sensitive data is more easily maintained.

Division B: Mandatory Protection contains three classes that are characterized by a Trusted Computing Base (TCB) that preserves the integrity of the security labels and uses them to enforce a set of mandatory access control rules by using the reference monitor concept (eg. a security kernel). These three classes are: Class B1: Labeled Security Protection, Class B2: Structured Protection, and Class B3: Security Domains.

Class B1 systems have all the same requirements found in Class C2. Additionally, an informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information and any flaws detected by testing must be corrected [Ref. 6:p. 20].

In contrast to Class B1, Class B2 requires the presence of a formal security policy clearly stating both mandatory and discretionary access controls. The TCB enforces a more rigid authentication mechanism. This is the first level that addresses covert channels - a

communication channel that allows the transfer of information in such a manner that violates the system's security policy. Systems conforming to Class B2 requirements are considered to be relatively resistant to penetration.

Class B3 must include a reference monitor that will mediate all user access to system information, be tamperproof, and be small enough for exhaustive tests and analysis. Security administration is supported and audit mechanisms are expanded to signal all security-relevant events with recovery procedures required. Class B3 systems are considered to be highly resistant to penetration.

Finally, Division A: Verified Design presently contains one class - Class A1: Verified Design which has the most rigid security requirements given the state of current technology. Extensive documentation is required on the TCB to demonstrate the ability to conform to security requirements. Systems in this class are functionally equivalent to Class B3. There are no architectural features or policy difference. The significant highlight is the added emphasis on formality in this class. Formal security verification methods are required to assure that both mandatory and discretionary access controls protect all classified or sensitive information either stored or processed on the trusted system.

Figure 3.1 [Ref. 6:p. 107] summarizes the trusted computer system evaluation criteria requirements for each classification.

TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA SUMMARY CHART

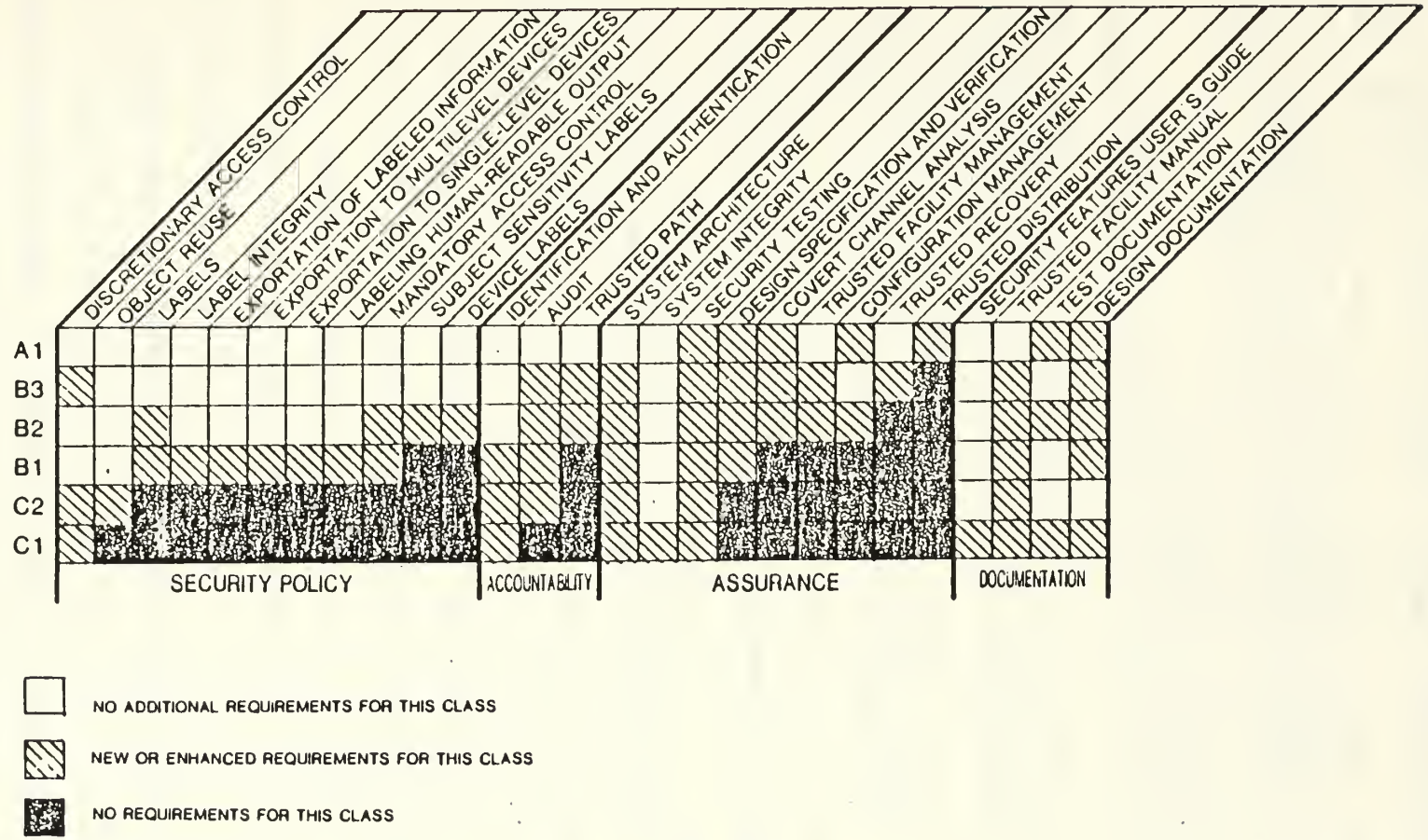

Figure 3.1 - Summary Chart

B. TRUSTED NETWORK SYSTEMS

The second DoD Computer Security Center publication previously mentioned currently exists in draft form only. The document is entitled, Department of Defense Trusted Network Evaluation Criteria, dated 29 July 1985, and is the logical complement to the DoD Trusted Computer System Evaluation Criteria.

The criteria were first established for computer systems in 1983, but it was soon realized that there were unique risks associated with distributed systems or networks that needed to be addressed separately.

Distributed computer systems or networks are composed of a set of nodes, communications lines connecting these nodes, and a set of rules (protocol) to facilitate the network's operation. A node is usually composed of a communications processor (switch) and at least one host processor. At one extreme, a single processor may serve both the communications and host functions. On the other, each function may be performed by multiprocessors. A typical node configuration may include a communications processor, a host, and a network front-end processor (NFEP) which may perform both pre- and post- processing for the host.

Establishing a security policy for a distributed system is a far greater task than in a centralized system. Security in the distributed system is only as strong as the quality of the enforced security policy at any one node and a breach of security at one node can have grave implications for other nodes in the system. An environment exists where users interact with host systems via remote access terminals in a real time fashion where data can be accessed, read, altered, or destroyed in a very rapid manner. Often these remote terminals are in a more hostile

environment than the host and the user is free from administrative and operational controls.

Certainly, the security issues of distributed systems are more than the union of the security issues of communications and computer systems. These issues address a unique threat of leakage or loss [Ref. 8:p. 30]:

1. The physical security problem extends beyond the physical environs of host computer's location.

2. The communications lines are vulnerable to tapping or passive monitoring of emanations. Crosstalk between communications lines or within the switching centrals can present a vulnerability.

3. A large population of users with varying clearances and need-to-know authorizations interact simultaneously on the network system.

4. The probability of system error and vulnerability to intrusion becomes greater as the size of the network increases.

5. Exhaustive testing and verification of software to determine if errors or anomalies exist is not possible for large software systems.

6. The identification of a user located at a remote terminal or facility is more difficult.

The Trusted Network Evaluation Criteria is divided into two parts: Trusted Network Criteria, applied on a global network-wide basis, and Trusted Network Component Criteria, applicable to individual network components. Both parts are closely linked and many of the criteria are derived from the "orange book."

Again, there are four hierarchical divisions of enhanced security protection. These divisions are delineated with respect to the three issues of data compromise, erroneous communications, and denial of service. Since different hardware and software are likely to be used

within network systems, a separate evaluation should be conducted in each area.

For a network to be assigned a division rating for data compromise, erroneous communications, or denial of service the network must satisfy all Trusted Network Criteria for that division and all of its trusted components must satisfy at least the equivalent division requirements of the Trusted Network Component Criteria. Limited by technology, criteria for erroneous communications and denial of service are yet to be defined for the most rigid security division, NA.

A reference model such as the International Standards Organization Open Systems Interconnection (OSI) Model or its equivalent must be established for comparison purposes when evaluating a network. "The hierarchy of protocols to be used within the network by host computers and network components must be specified, as well as the location and content of any security-relevant information contained within those protocols, such as security labels. A direct correspondence must be shown between the security-relevant portions of these communications protocols and the security features employed in the trusted components." [Ref. 7:p. 4]

1. Fundamental Requirements

The six fundamental requirements listed previously for a "secure" computer system can be extended for applicability to the "secure" network with little modification - four dealing with what needs to be done to control security in a trusted network and two dealing with credible assurances that these requirements are met.

2. The Criteria

Again, the Trusted Network Criteria define the minimum set of global security features and assurance requirements to be met by the Trusted Network Base (TNB). There are many parallels between the four hierarchical divisions of the Trusted Network Criteria and the Trusted Computer Systems Evaluation Criteria. The four divisions are Division ND, Division NC, Division NB, and Division NA. Significant additions having relevancy to trusted network systems will be discussed.

Division ND: Minimal Protection is reserved for those systems that have been evaluated but failed to meet the requirements for a higher evaluation division. Minimum security results and there are no security features to protect against data compromise, erroneous communications, and denial of service.

Minimal data compromise, erroneous communications, and denial of service are indicative of **Division NC: Controlled Access Protection**. Security decisions based on the classification of information are handled administratively; thus, networks within this division are not required to make security decisions based on the classification of objects and subjects. Network compromise protection is achieved through the use of techniques such as resource isolation within network components, data encryption, or physical protection of the communications medium. Network discretionary access control is defined by the Trusted Network Base (TNB) and uses enforcement mechanisms such as closed user groups and network access control lists to include or exclude access with the focus on the single network subject. The following documentation is also required for this division: Network

Security Features User's Guide, Trusted Network Facility Manual, Network Test Documentation, and Network Design Documentation.

A documented, formal security policy model that requires mandatory access control enforcement over all network subjects and network objects and which addresses the issue of covert channels must exist for networks within **Division B: Mandatory Protection**. TNB design and implementation require more thorough testing and more complete review. The TNB must maintain sensitivity labels for all network resources that can be accessed either directly or indirectly by subjects external to the TNB. These labels are to be used as the basis for access control decisions. "The TNB shall support a trusted communication path between network subjects for use when positive component to component communication is required (e.g., initialization, encryption key management, change of network subject security level(s)). Communications via this trusted path shall be activated exclusively by a network subject or the TNB and shall be logically and unmistakably distinguishable from other paths." [Ref. 7:p. 19] The same documents are required as in the previous level; however, a more formal description of the network's resources and test results is needed.

Division NA: Verified Design requires networks to possess a reference monitor that mediates all accesses of subjects to objects, be tamperproof, and the distributed portions of the TNB to be small enough to be subjected to analysis and tests. Formal design specification and verification techniques assure that the TNB is correctly implemented. There are two types of formal specification - "formal policy model" and "formal top level specification (FTLS)". The "formal policy model" is

used to analyze a complete network and must be demonstrated by a mathematical proof that it supports the security policy. The "formal top level specification (FTLS)" deals with the detailed functionality of the network and must be consistent with the model by formal verification techniques. Formal analysis techniques must be used to identify and analyze covert channels.

The Trusted Network Component Criteria are detailed to establish the minimum set of security features and assurance requirements that each component must meet in order to insure that the global Trusted Network Base (TNB) requirements can be achieved. These standards are treated in the same manner as the aforementioned Trusted Network Criteria; thus, little purpose is served by pointing out the specific requirements of each division (see Reference 7 for more details).

IV. RISK ASSESSMENT

The purpose of multilevel security is to provide cost-effective countermeasures to protect a system from the many threats which exist. These countermeasures must reduce the frequency and impact of threats upon the system, provide for contingency planning when the system's operation is disrupted, and audit the system in both the normal and standby modes of operation. The problem of weighing the risk of the loss threatened with the cost of effective countermeasures gives rise to the imprecise science of risk management. A brief discussion of risk management in general will be followed by a look at the methodology set forth by the DoD Computer Security Center for assessing a system's inherent risk and at an approach suggested by Carl Landwehr and H. O. Lubbes of the Naval Research Laboratory in Washington, D.C.

A. RISK MANAGEMENT

Risk management involves the manipulation of various tools and techniques tailored to meet a specific need in the prevention of unauthorized intervention in the various levels of a system's operation. However, the methodologies employed are basic [Ref. 9:p. 26]:

a. Threat identification

b. Threat impact measurement

c. Countermeasure identification and measurement

d. Countermeasure selection

e. Implementation and monitoring of safeguard effect

Historically, risk managers have measured the cost-effectiveness of security measures taken in terms of dollars. This has led to greater concern over those threats that cause total or near total destruction of the system (e.g., natural causes, gross errors, omissions). If reasonable security measures have been taken, many of these threats (e.g., errors and omissions) have a greater probability of occurrence than penetration of the system by an unauthorized source . It is also difficult to determine the "cost" of compromised classified information (assuming that a penetration has been detected). However, once the commitment is made to develop multilevel trusted systems, greater access to systems by users of varying levels of clearances and need-to-know authorizations increase the risk of compromise. The need still exists for safeguards against the traditional concerns, but the threat of unauthorized penetration must be given much greater attention when the secrets of a nation are at stake. The DoD Computer Security Center has developed a scheme for assessing the risk in trusted systems.

B. RISK INDEX

The evaluation classes described in the DoD Trusted Computer System Evaluation Criteria are primarily based on the level of security risk inherent to a particular system. Another DoD Computer Security Center publication, Technical Rationale Behind CSC-STD-003-85: Computer Security Requirements--Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, presents a methodology for assessing a system's inherent risk - the "risk index." "The risk index can be defined as the disparity between the minimum clearance or authorization of system users and the maximum

sensitivity of data processed by a system." [Ref. 10:p. 5] Although other factors can influence security risk, the risk index is uniformly applied in the determination of security risk and is the only basis for determining the minimum class of trusted systems.

The risk index is computed by comparing the system's minimum user clearance (R_{min}) from Table 4.1 [Ref. 10:p. 6] with the system's maximum data sensitivity (R_{max}) from Table 4.2 [Ref. 10:p. 7]. The relationships for the actual computations follow:

Case I. If R_{min} is less than R_{max} then the Risk Index is determined by subtracting R_{min} from R_{max}:

$$\text{Risk Index} = R_{max} - R_{min}$$

(This equation works in all cases but one. When the minimum clearance is Top Secret/Background Investigation and the maximum data sensitivity is Top Secret, the Risk Index should be 0 rather that the computed value of 1.)

Case II. If R_{min} is greater than or equal to R_{max}, then:

Risk Index = | 1, if there are categories on the system to which some of the users are not authorized access.

Risk Index = | 2, otherwise (i.e., if there are no categories on the system or if all users are authorized access to all categories).

Table 4.3 [Ref. 10:p. 8] is a matrix of computed security risk indexes for categories associated with maximum data sensitivity levels above Secret. If local authorities feel that the environment has additional risk factors affecting system security, a larger risk index can be assigned.

TABLE 4.1

RATING SCALE FOR MINIMUM USER CLEARANCE[1]

MINIMUM USER CLEARANCE	RATING (R_{min})
Uncleared (U)	0
Not Cleared but Authorized Access to Sensitive Unclassified Information (N)	1
Confidential (C)	2
Secret (S)	3
Top Secret (TS)/Current Background Investigation (BI)	4
Top Secret (TS)/Current Special Background Investigation (SBI)	5
One Category (1C)	6
Multiple Categories (MC)	7

[1]See Apppendix B for a detailed description of the terms listed

TABLE 4.2

RATING SCALE FOR MAXIMUM DATA SENSITIVITY

MAXIMUM DATA SENSITIVITY RATINGS[2] WITHOUT CATEGORIES (R_{max})	RATING (Rmax)	MAXIMUM DATA SENSITIVITY WITH CATEGORIES[1]	
Unclassified (U)	0	Not Applicable[3]	
Not Classified but Sensitive[4]	1	N With One or More Categories	2
Confidential (C)	2	C With One or More Categories	3
Secret (S)	3	S With One or More Categories With No More Than One Category Containing Secret Data	4
		S With Two or More Categories Containing Secret Data	5
Top Secret (TS)	5[5]	TS With One or More Categories With No More Than One Category Containing Secret or Top Secret Data	6
		TS With Two or More Categories Containing Secret or Top Secret Data	7

[1]The only categories of concern are those for which some users are not authorized access to the category. When counting the number of categories, count all categories regardless of the sensitivity level associated with the data. If a category is associated with more than one sensitivity level, it is only counted at the highest level.

[2]Where the number of categories is large or where a highly sensitive category is involved, a higher rating might be warranted.

[3]Since categories imply sensitivity of data and unclassified data is not sensitive, unclassified data by definition cannot contain categories.

[4]N data includes financial, proprietary, privacy, and mission sensitive data. Some situations (e.g., those involving extremely large financial sums or critical mission sensitive data), may warrant a higher rating. The table prescribes minimum ratings

[5]The rating increment between the Secret and Top Secret data sensitivity levels is greater than the increment between other adjacent levels. This difference derives from the fact that the loss of Top Secret data causes exceptionally grave damage to the national security, whereas the loss of Secret data causes only serious damage.(4)

TABLE 4.3

SECURITY RISK INDEX MATRIX

Maximum Data Sensitivity

Minimum Clearance or Authorization of System Users	U	N	C	S	TS	1C	MC
U	0	1	2	3	5	6	7
N	0	0	1	2	4	5	6
C	0	0	0	1	3	4	5
S	0	0	0	0	2	3	4
TS(BI)	0	0	0	0	0	2	3
TS(SBI)	0	0	0	0	0	1	2
1C	0	0	0	0	0	0	1
MC	0	0	0	0	0	0	0

U = Uncleared or Unclassified
N = Not Cleared but Authorized Access to Sensitive Unclassified Information or Not Classified but Sensitive
C = Confidential
S = Secret
TS = Top Secret
TS(BI) = Top Secret (Background Investigation)
TS(SBI) = Top Secret (Special Background Investigation)
1C = One Category
MC = Multiple Categories

C. SECURITY ENVIRONMENT

As mentioned previously, factors other than the risk index are important when the overall threat of compromised information is to be considered. One such factor is the nature of the environment in which the system is operating. The environment is the aggregate of external factors affecting the development, operation, and maintenance of a system. Two common environments referred to are the open and the closed environment. This description is based upon the TCB's vulnerability to the insertion of malicious logic. Malicious logic can be either hardware, software, or firmware that is intentionally included in a system for the express purpose of causing loss or harm. An open environment is one in which adequate precautions against the insertion of malicious logic have not been invoked. Conversely, a closed environment is one that is considered to be adequately protected against such threats.

1. Open Security Environment

An open security environment exists when either of the following conditions holds true:

a. Application developers (including maintainers) do not have sufficient clearance (or authorization) to provide an acceptable presumption that they have not introduced malicious logic. Sufficient clearance is defined as follows: where the maximum classification of data to be processed is Confidential or below, developers are cleared and authorized to the same level as the most sensitive data; where the maximum classification of data to be processed is Secret or above, developers have at least a Secret clearance.

b. Configuration control does not provide sufficient assurance that applications are protected against the introduction of malicious logic prior to or during the operation of system applications. [Ref. 10:p. 31]

In the open security environment, the application of malicious logic can affect the TCB in two ways. The first way is an attack on TCB controls in an attempt to "penetrate" the system. Secondly, any covert channels that exist in the TCB can be exploited.

Table 4.4 presents the minimum evaluation class identified in the Computer Security Requirements for different risk indices in an open security environment [Ref. 10:p. 12]. Table 4.5 illustrates the impact of the requirements on individual minimum clearance/maximum data sensitivity pairings, where no categories are associated with maximum data sensitivity below Top Secret [Ref. 10:p. 13]. The classes obtained from these tables reflect minimum values. Again, if the environment dictates, the assignment of a higher class may be warranted. Two factors that may lead to a higher class assignment are: a) High volume of information at the maximum data sensitivity, and b) Large numbers of users with minimum clearance. These two factors are common in networks.

Systems operating in a system high or dedicated mode have a risk index of zero. A system operating in the dedicated mode is characterized by all users having the appropriate clearance and need-to-know requirements for all information on the system. Strictly speaking, no additional requirements exist for hardware or software to enforce the security policy; however, such features may be necessary because of the integrity and denial of service requirements for many systems.

A system operating in the system high mode, is characterized by all users having the appropriate clearance but not the need-to-know for all information on the system. Obviously, discretionary measures are

TABLE 4.4

COMPUTER SECURITY REQUIREMENTS FOR OPEN SECURITY ENVIRONMENTS

RISK INDEX	SECURITY OPERATING MODE	MINIMUM CRITERIA CLASS[1]
0	Dedicated	No Prescribed Minimum[2]
0	System High	C2[3]
1	Limited Access, Controlled, Compartmented, Multilevel	B1[4]
2	Limited Access, Controlled, Compartmented, Multilevel	B2
3	Controlled, Multilevel	B3
4	Multilevel	A1
5	Multilevel	*
6	Multilevel	*
7	Multilevel	*

[1]The asterisk (*) indicates that computer protection for environments with that risk index are considered to be beyond the state of current technology. Such environments must augment technical protection with personnel or administrative security safeguards.

[2]Although there is no prescribed minimum, the integrity and denial of service requirements of many systems warrant at least class C1 protection.

[3]If the system processes sensitive or classified data, at least a class C2 system is required. If the system does not process sensitive or classified data, a class C1 system is sufficient.

[4]Where a system processes classified or compartmented data and some users do not have at least a Confidential clearance, or when there are more than two types of compartmented information being processed, at least a class B2 system is required.

TABLE 4.5

SECURITY INDEX MATRIX FOR OPEN SECURITY ENVIRONMENTS[1]

Maximum Data Sensitivity

Minimum Clearance or Authorization of System Users	U	N	C	S	TS	1C	MC
U	C1	B1	B2	B3	*	*	*
N	C1	C2	B2	B2	A1	*	*
C	C1	C2	C2	B1	B3	A1	*
S	C1	C2	C2	C2	B2	B3	A1
TS(BI)	C1	C2	C2	C2	C2	B2	B3
TS(SBI)	C1	C2	C2	C2	C2	B1	B2
1C	C1	C2	C2	C2	C2	C2[2]	B1[3]
MC	C1	C2	C2	C2	C2	C2[2]	C2[2]

[1]Environments for which either C1 or C2 is given are for systems that operate in system high mode. No minimum level of trust is prescribed for systems that operate in dedicated mode. Categories are ignored in the matrix, except for their inclusion at the TS level.

[2]It is assumed that all users are authorized access to all categories present in the system. If some users are not authorized for all categories, then a class B1 system or higher is required.

[3]Where there are more than two categories, at least a class B2 system is required.

U = Uncleared or Unclassified
N = Not Cleared but Authorized Access to Sensitive Unclassified Information or Not Classified but Sensitive
C = Confidential
S = Secret
TS = Top Secret
TS(BI) = Top Secret (Background Investigation)
TS(SBI) = Top Secret (Special Background Investigation)
1C = One Category
MC = Multiple Category

needed to protect information from those users without the appropriate need-to-know. At least a Class C2 system is required because of its accountability capabilities when systems process and/or store classified or sensitive unclassified data. If the maximum sensitivity of the data is unclassified, a Class C1 system is acceptable. No audit trails are traceable to the individual, but protection is still needed to protect project or private information and to prevent the accidental reading or destruction of another user's data.

A risk index of 1 or higher is characteristic of systems operating in controlled, compartmented, and multilevel modes. In these modes, mandatory access control to objects is usually controlled by the use of sensitivity labels. Mandatory access controls are inherent to Division A and B systems and are required for all environments with risk indices of 1 or greater. The minimum class recommended for systems requiring mandatory access control is Class B1.

Systems with a risk index of 2 require more trust than is afforded by the Class B1 system. Where a sensitivity label alone exists (no label denoting category), Class B2 systems are the minimum requirement for minimum clearance/maximum data sensitivity pairings such as U/C, N/S, and S/TS.

Although Class B2 systems are relatively resistant to penetration, a risk index of 3 requires even greater resistance to penetration such as that demonstrated by a Class B3 system. Class B3 systems are the minimum requirement for minimum clearance/maximum data sensitivity pairings of U/S, C/TS, S/TS with one category and TS(BI)/TS with multiple categories.

The most trustworthy systems at the present time are Class A1 systems. Class A1 systems are to be used for situations with a risk index of 4 and are the minimum requirement for minimum clearance/maximum data sensitivity pairings of N/TS, C/TS with one category, and S/TS with multiple categories. Formal design specification and verification techniques distinguish Class A1 from Class B3 (the architecture and policy requirements are the same).

Any system operating in an environment with a risk index of 5 or greater cannot be made trustworthy with current technology. An open environment with uncleared users and Top Secret data is not permissible under any conditions.

2. Closed Security Environment

A closed security environment is protected from the insertion of malicious logic; however, a threat to the TCB exists from the exploitation of unintentional errors in logic for malicious purposes. A closed security environment exists when both of the following conditions hold true:

a. Applications developers (including maintainers) have sufficient clearances and authorizations to provide an acceptable presumption that they have not introduced malicious logic.

b. Configuration control provides sufficient assurance that applications are protected against the introduction of malicious logic prior to and during the operation of system applications. [Ref. 10:p. 32]

Clearances are required for assurance against malicious applications logic because there are relatively few tools for assessing the security-relevant behavior of application hardware and software. The DoD Computer System Evaluation Criteria outline assurance

requirements such as extensive functional testing, penetration testing, and correspondence mapping between a security model and the design for increased confidence in the TCB.

In the closed security environment, a Class B2 system is the result of adherence to requirements that are rigid enough to substantially reduce the number of unintentional errors in logic and is worthy of increased trust. A system evaluated as a Class B1 system in an open security environment cannot be degraded to a Class C1 or C2 system in a closed security environment because of the requirement for mandatory access controls.

Table 4.6 presents the minimum evaluation class identified in the Computer Security Requirements for different risk indices in a closed security environment [Ref. 10:p. 20]. The principal difference between the open and closed security environments is that Class B2 systems in the closed security environment are trusted to provide sufficient protection for a greater risk index. Table 4.7 illustrates the requirement's impact on individual minimum clearance/maximum data sensitivity pairings [Ref. 10:p. 21]. Unlike the open security environment, protection support for some closed environments, such as an uncleared user on a system processing Top Secret data, is allowed.

D. ANOTHER APPROACH FOR RISK ASSESSMENT

Carl Landwehr and H. O. Lubbes feel that the DoD Computer Security Center did an outstanding job of defining requirements corresponding to specified levels of security functions and assurance. However, the technical guidance provided falls short of adequately providing guidance for what level of system is appropriate in a given environment. They

TABLE 4.6

COMPUTER SECURITY REQUIREMENTS FOR CLOSED SECURITY ENVIRONMENTS

RISK INDEX	SECURITY OPERATING MODE	MINIMUM CRITERIA CLASS[1]
0	Dedicated	No Prescribed Minimum[2]
0	System High	C2[3]
1	Limited Access, Controlled, Compartmented, Multilevel	B1[4]
2	Limited Access, Controlled, Compartmented, Multilevel	B2
3	Controlled, Multilevel	B2
4	Multilevel	B3
5	Multilevel	A1
6	Multilevel	*
7	Multilevel	*

[1]The asterisk (*) indicates that computer protection for environments with that risk index are considered to be beyond the state of current technology. Such environments must augment technical protection with physical, personnel, and/or administrative safeguards.

[2]Although there is no prescribed minimum, the integrity and denial of service requirements of many systems warrant at least class C1 protection.

[3]If the system processes sensitive or classified data, at least a class C2 system is required. If the system does not process sensitive or classified data, a class C1 system is sufficient.

[4]Where a system processes classified or compartmented data and some users do not have at least a Confidential clearance, at least a class B2 system is required.

TABLE 4.7

SECURITY INDEX MATRIX FOR CLOSED SECURITY ENVIRONMENTS[1]

Minimum Clearance or Authorization of System Users	Maximum Data Sensitivity: U	N	C	S	TS	1C	MC
U	C1	B1	B2	B2	A1	*	*
N	C1	C2	B1	B2	B3	A1	*
C	C1	C2	C2	B1	B2	B3	A1
S	C1	C2	C2	C2	B2	B2	B3
TS(BI)	C1	C2	C2	C2	C2	B2	B2
TS(SBI)	C1	C2	C2	C2	C2	B1	B2
1C	C1	C2	C2	C2	C2	C2[2]	B1[3]
MC	C1	C2	C2	C2	C2	C2[2]	C2[2]

[1]Environments for which either C1 or C2 is given are for systems that operate in system high mode. There is no prescribed minimum level of trust for systems that operate in dedicated mode. Categories are ignored in the matrix, except for their inclusion at the TS level.

[2]It is assumed that all users are authorized access to all categories on the system. If some users are not authorized for all categories, then a class B1 system or higher is required.

[3]Where there are more than two categories, at least a class B2 system is required.

U = Uncleared or Unclassified
N = Not Cleared but Authorized Access to Sensitive Unclassified Information or Not Classified but Sensitive
C = Confidential
S = Secret
TS = Top Secret
TS(BI) = Top Secret (Background Investigation)
TS (SBI) = Top Secret (Special Background Investigation)
1C = One Category
MC = Multiple Categories

feel that the scheme described above is still not enough in assessing the Navy's security needs. Their apprehension can certainly be extended to the entire military community.

In their paper, An Approach to Determining Computer Security Requirements for Navy Systems, Landwehr and Lubbes describe a method for applying the Orange Book to represenative large-scale dispersed systems seen in the Navy and propose a system of looking at risk factors not previously addressed in DoD literature pertaining to trusted systems. They also propose a scheme for applying these risk factors to assess a system's overall risk which in turn will be the basis for the security requirements of that system. A discussion of their ideas follow.

1. Applying Security Requirements

A method of applying the computer security requirements in the Orange Book to trusted systems is depicted in Figure 4.1 [Ref. 11:p. 3] and defined below:

a. extracting from each system (or system design) the factors that affect the risk that its operation may lead to the unauthorized disclosure of sensitive information,
b. quantifying these factors, and
c. determining system security requirements (in terms of the levels defined in the Orange Book) that reduce the system risk to an acceptable level. [Ref. 11:p. 2]

This method qualifies as a risk evaluation since the threat of unauthorized disclosure of sensitive information exists. The system risk is a mix of the value of the system's assets (sensitive information), the system's vulnerabilities, and the clearance of the users.

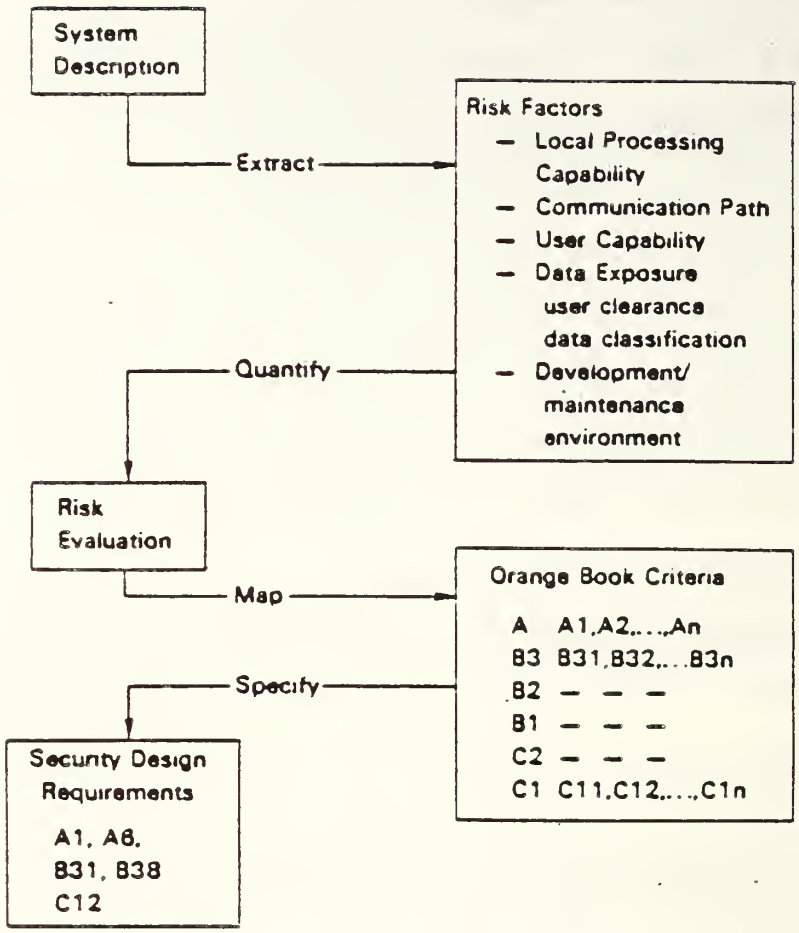

Figure 4.1 - Steps in Applying Guidance

2. Identifying the Risk Factors

Landwehr and Lubbes propose several new classes of risk factors that affect actual system risk - local processing capability, communication path, user capability, development/maintenance environment, and data exposure. Within each of these classes is a list of independent risk levels that represent a comparable increase or decrease in risk between adjacent levels.

Local processing capability addresses the capabilities of the user's terminal. Capabilities range from the receive-only terminal (no system commands can be entered directly) to the fixed-function interactive terminal (allows both sending and receiving information) to the programmable terminal (can be programmed to enter commands). The programmable terminal introduces the highest level of risk and is the equivalent of using a personal computer as a terminal. The identified risk levels for local processing capability are:

Level 1: receive-only terminal

Level 2: fixed-function interactive terminal

Level 3: programmable device (access via personal computer or programmable host)

The communications path between the terminal and the host also affects the level of risk in the system. The lowest risk level exists in terminal that has a simplex receive-only link to its host via store-and-forward (S/F) network (e.g., fleet broadcast). Terminals connected to the host directly, through a local-area network, or a long-haul network such as DDN typify the greatest risk of penetration because of the increased bandwidths and closer host-terminal

interactions common to these systems. The identified risk levels for communications path are:

Level 1: store/forward, receive-only

Level 2: store/forward, send/receive

Level 3: interactive (I/A), via direct connection, local-area net, or long-haul packet net

A system that allows only certain predefined inputs is less risky than a system that responds to user transactions. Succinctly stated, limiting the user's capabilities lessens the system risk. The identified risk levels for user capability are:

Level 1: output only

Level 2: transaction processing

Level 3: full programming

A system that is developed and maintained by cleared individuals (commonly seen in the intelligence community) represents a lower risk level than the majority of systems that are developed and maintained without this requirement. Using this assumption, Landwehr and Lubbes consider all systems to have been developed and maintained as the majority, in an open environment. Therefore, no risk levels are identified for the development/maintenance environment.

The greater the disparity between the clearance of the least-cleared user and the classification of the most sensitive data stored or processed by the system, the greater the risk. This class is similar to that stated above by the DoD Computer Security Center, but it is termed data exposure to distinguish it from other risk factors. Clearance levels are identified as:

Level 0: uncleared

Level 1: uncleared, but authorized access to sensitive classified information

Level 2: confidential clearance

Level 3: secret clearance

Level 4: top secret/background investigation

Level 5: top secret/special background investigation

Level 6: top secret/special background investigation, with authorization for one compartment

Level 7: top secret/special background investigation, with more than one compartment

Classification levels are numbered:

Level 0: unclassified

Level 1: sensitive unclassified information

Level 2: confidential

Level 3: secret

Level 4: secret with one category

Level 5: top secret with no categories, or secret with two or more categories

Level 6: top secret with one category

Level 7: top secret with two or more categories

Data exposure is computed as the difference between the level of the least-cleared user of a system and the maximum level of data processed by the system. The range of values is from 0 (all users cleared for all data) to 7 (uncleared users with information being processed that is top secret with two or more categories).

3. Applying the Risk Factors

Once the various risk levels have been determined for a particular system, Tables 4.8, 4.9, and 4.10 are used to provide the necessary mappings between factor values, risk factor levels, and security requirements as presented in the Orange Book. Local processing capability and communication path provide the basis for the process coupling risk - the degree to which a process can maintain its integrity when subjected to subversion from an outside source (Table 4.8). A close degree of interaction results in a high degree of coupling which yields to increased vulnerability. Coupling the process coupling risk with user capability yields an overall system risk that is independent of the data exposure (Table 4.9). The security requirement is read from Table 4.10 as the result of relating overall system risk and data exposure. As stated previously by the DoD Computer Security Center, system requirements are not technically feasible at this time for all situations.

This technique is superior to that of the DoD Computer Security because a broader range of threats are specifically addressed. System requirements can still be upgraded if the environment appears to pose unique threats that have not been addressed. Landwehr and Lubbes point out that approaches for determining other security requirement (e.g., TEMPEST, degaussing, COMSEC, contingency planning) are beyond the scope of their approach.

TABLE 4.8 - PROCESS COUPLING RISK

Local Processing Capability	Communication Path		
	1. S/F Net (one-way)	2. S/F Net (two-way)	3. I/A Net or Direct Connection (LAN,DDN)
1. Receive-only terminal	2[1]	3	4
2. Interactive terminal (fixed function)	2	4	5[2,4]
3. Programmable device (Access via personal computer or programmable host)	4	5	6[3]

TABLE 4.9 - SYSTEM RISK

User Capability	Process Coupling Risk				
	2	3	4	5	6
1. Output-only (subscriber)	3[1]	4	5	6	7
2. Transaction processing	—	5	6	7[2]	8
3. Full programming	—	6	7	8[4]	9[3]

TABLE 4.10 - MAPPING SYSTEM RISK AND DATA EXPOSURE TO ORANGE BOOK LEVELS

Data Exposure	System Risk						
	3	4	5	6	7	8	9
0	C1	C1	C1	C1/C2	C2[2]	C2	C2
1	C1/C2	C2	C2	C2	C2/B1	B1	B1
2	C2	C2/B1	B1	B1	B1	B1/B2[4]	B2[3]
3	B1	B1	B1/B2	B2	B2/B3	B3	B3/A1
4	B2[1]	B2/B3	B3	B3/A1	A1	A1	A1
5	B3/A1	A1	A1	—	—	—	—
6	—	—	—	—	—	—	—
7	—	—	—	—	—	—	—

V. MULTILEVEL SECURITY IN THE W.A.R. LAB

One of the main purposes of this paper is to investigate the integration of the Gemini Trusted Multiple Microcomputer Base into the Wargaming, Analysis, and Research (W.A.R.) Lab. Currently, the acquisition process for a Gemini system has begun with an estimated delivery date in May 1986. Primarily, the system is being purchased to become the basis for research involving multilevel security; however, it is worthwhile to search for other applications that can enhance or upgrade the current security posture in the W.A.R. lab.

A. THE W.A.R. LAB

In 1977, the Wargaming, Analysis, and Research Lab received sponsorship from the Defense Advanced Projects Research Agency (DARPA) as a research center for topics involving command, control, and communications (C3). Two years later, the lab opened with a PDP-11/70 computer and GENESCO graphics. Today, the laboratory is a modern, TEMPEST-hardened facility with significant information processing and storage capability. Appendix C details the current systems/software available in the W.A.R. lab.

The W.A.R. lab is currently used for wargaming, classified thesis preparation, course projects, and research activities. The facility is of prime importance in the USREDCOM's development of the Joint Theater Level Simulation (JTLS) development. Also, controlled experiments in

headquarters effectiveness are conducted periodically by the Defense Communications Agency (DCA).

There are three different wargaming and simulation courses taught twice each academic year at the Naval Postgraduate School. These courses involve approximately 160 students from seven curriculums - OR, C^3, ASW, EW, Space Ops, Air Ocean Tactical Environment Support, and NSA. The instruction provided to officer students covers full and limited exposure to wargaming, mathematical modeling and simulation techniques, decision theory, validation of models, and design of experiments. Thesis and professional research cover such diverse areas as red side planning models, ASW modeling and computer simulation, computer graphics enhancements, Interactive Battle Group Tactical Trainer (IBGTT) and Naval Warfare Gaming System (NWGS) model validation, distributed computing with large and small networks, and voice input devices and techniques.

B. THE GEMINI TRUSTED MULTIPLE MICROCOMPUTER BASE

The Gemini Trusted Multiple Microcomputer system is a product of Gemini Computers, Incorporated of Monterey, California. Up to eight iAPX286-based microcomputers can be modularly connected on the same Multibus to provide a combination of multilevel security and multiprogramming capabilities. The system can provide a trusted base for both concurrent and real-time applications such as command, control, communications, intelligence, weapons, networks, and office automation.

The Gemini system includes the Gemini bus controller, a real-time clock with battery, and data encryption device using the standard NBS-DES algorithm. Non-volatile memory is used for storing passwords

and secret encryption keys. The Gemini computer system supports the following programming languages: Pascal MT+, JANUS ADA, PL/1, C, and Fortran.

The iAPX286 microprocessor combines the central processing unit and the memory management unit on the same chip. This microprocessor supports four hierarchical privilege levels for protection and mediation of all memory and I/O references.

The Gemini Multiprocessing Secure Operating System (GEMSOS) stores all information in discrete logical objects called segments. These segments are managed with respect to their security access class and access mode. GEMSOS supports both sensitivity and integrity access classes (each with 8 levels and 24 compartments) for mandatory security policies. Discretionary security policies are also enforced on an application-specific basis.

For additional information on the Gemini Trusted Multiple Microcomputer Base, refer to Appendix C for a product description (quoted from an information packet from Gemini Computers, Inc).

C. RISK ASSESSMENT IN THE W.A.R. LAB

This risk assessment will only take into account those areas most applicable to the multilevel secure environment.

1. Current Assessment

As mentioned previously, the W.A.R. lab operates in the "system-high" security mode. All personnel that are authorized access to the facility must possess a Secret clearance as a minimum and the highest classification of information stored or processed by all mainframe computers and microcomputers is also Secret. The only

discrepancy existing between the users' minimum clearance and the maximum data sensitivity of information stored or processed in the lab is that of need-to-know. Obviously, selective exposure to classified material is desired and the list of those who should have access to all information resident in the facility is small. Passwords to directories and files are the only safeguard for discretionary dissemination of data and their compromise can result from the crowded conditions that often exist in the lab. Along with the problem of material being viewed by those who should not have discretionary access, a greater threat of unintentional or malicious tampering of either programs or data exists.

At the present time the only I/O external to the physical confines of the lab is a secure link to the USREDCOM at McDill AFB in Florida. Data link encryption is provided by a crypto generator (KG-34).

2. Proposed W.A.R. Lab Operations

Before proceeding further with a look at risk assessment, it is necessary to detail some of the possible options for configuration (minimum user clearance/maximum data sensitivity) that would be optimal for utilization of the facility. These proposed configurations are made on the basis of three assumptions: the lab remains at its current location in Room 157, Ingersoll Hall; the lab's role as a research and a teaching facility remains unchanged; and the highest classification of information being stored or processed in order to fulfill its assigned role continues to be Secret.

Option 1. The lab continues to operate in the "system-high mode", but with greater attention towards isolating various levels of

information within the lab. This option could be effectively implemented without the introduction of new hardware. By using existing room dividers to create cells for specific "types" of work, the effectiveness of the current password security would be greatly enhanced by reducing the risk of accidental compromise. However, such an implementation would be impractical because of the overcrowding that often exists in the lab. During the conduct of wargames, the entire facility is used and participants are often required to move freely between cells.

With the introduction of the Gemini Trusted Multiple Microcomputer Base, selected material can be processed and stored by the system's Trusted Computing Base (TCB) with access being granted only to those truly authorized. Such material can be routed to previously specified terminals only. Again, this is not a fix to the current situation in the lab, but rather, an alternative for that material which truly deserves discretionary isolation. For reasons that will be explained later, not all information that is processed or stored on the current mainframes can benefit from the discretionary access provided by the Gemini Computer.

Any system providing multilevel security or secure guard in the above situation (both open and closed environments) must be rated Class C2 as a minimum. Discretionary access is provided by Class C2 systems and such a rating is the minimum for any system that processes sensitive or classified information.

Option 2. The lab continues to operate in a "system-high" mode with increased emphasis on discretionary isolation. To alleviate the

frequent overcrowded conditions, an additional room has been physically secured elsewhere in Ingersoll Hall. Personnel who are not directly involved in wargaming can conduct research or assignments outside the W.A.R. lab proper.

Most of the comments stated concerning Option 1 are applicable to this configuration. Again, a system with a rating of Class C2 is sufficient for establishing a multilevel secure or guard environment. An additional consideration is the method or medium by which sensitive information is sent to the add-on work area. Physical security of the transmission medium or data encryption is required to prevent possible compromise.

Local processing capability and user capability can be tailored for each terminal allowing varying degrees of interaction with the host computer. Such complicating factors lend greater support for the proposed risk assessment scheme by Landwehr and Lubbes. Their scheme examines the risk level for more factors than that of the DoD Computer Security Center. In this case, a system with a rating of Class C2 is still considered adequate.

The same caveat applies as before. Not all information stored or processed by the current lab's mainframe computers will benefit from the discretionary access controls enforced by the Gemini computer.

Option 3. This option is the most ambitious and desirable of all the options presented. The computer security environment in the W.A.R. lab is one of total multilevel security. Terminals are available outside of the facility (classrooms, workspaces, and offices) for various levels of work utilizing the lab's resources. In secure and

unsecure workspaces, the local processing capability and the user capability of each terminal is tailored to meet specific requirements as in Option 2. Uncleared users may even be given authorization to use terminals that are placed in unsecure workspaces.

If these capabilities existed in the current lab, overcrowding would no longer be a problem. Students could enter the unclassified portions of their papers outside the lab. Instructors could set parameters for upcoming wargames in the convenience of their office. Classroom instruction could be conducted outside of the facility. Also, the lab's role could be enhanced greatly. Allied students would be able to participate in ongoing classified wargames since all sensitive material would be removed prior to display on a terminal designated for uncleared users. Instruction requiring the lab's resources would not be limited to those with appropriate clearances. Many more examples could be cited.

The application of the Computer Security Center's approach to risk assessment requires the minimum criteria class for a system that can support the configuration stated in Option 3 is Class B3 for the open environment and Class B2 for the closed environment. Again, the Landwehr and Lubbes scheme is more appropriate. If one chooses the factor yielding the lowest risk levels for each category (e.g., a receive-only terminal, S/F Net (one-way), user output only), it is possible to have a Class B1 system. Given the constraints leading to the low risk levels, the configuration of Option 3 can be realized with an unbearably low effectiveness. A Class B3 system is required when the factors yielding the greatest risk level for each category is selected.

The Computer Security scheme assumes maximum risk and does not enumerate the various factors. The Landwehr and Lubbes scheme evaluates the various factors, giving more flexibility in configuration design.

The Gemini Trusted Multiple Microcomputer Base is currently undergoing final evaluation for the Class B3 rating. It was developed as a "bolt-on" system to provide multilevel security, but will its integration into the W.A.R. lab produce the ambitious results needed to realize the configuration stated in Option 3?

D. INTEGRATION OF THE GEMINI COMPUTER INTO THE W.A.R. LAB

The Gemini Trusted Multiple Microcomputer Base can serve merely as a secure guard or can be the basis for a total multilevel secure environment.

1. The Gemini Computer as a Secure Guard

The role of a secure guard system is very similar to that of a multilevel secure system. The major function of both is to allow subjects of different levels of classification to operate on a common computer system or network. All of the above options present situations that require guard technology - mandatory and discretionary access.

The Gemini computer's TCB is responsible for insuring that only authorized subjects have access to information stored and processed on the system. The system has the capability of both storing and processing. A digital signature (label) placed on each object determines which subjects ultimately have access and the terms of that access. It is clear that all information created, stored, or processed on the Gemini system can be manipulated in the multilevel secure environment. However, when the Gemini system is integrated with the

existing computers in the lab, this integrity cannot necessarily be insured.

Since existing computers in the lab do not have a TCB, resident software cannot legitimately label objects and access by subjects (especially processes) to existing labelled objects cannot be tolerated. Therefore, in order to maintain information integrity, the only allowable integration of the Gemini system with existing computer systems in the lab is with partitioned memory sections on these existing systems. All information flow that is under the umbrella of the guard interface must go through the Gemini computer for routing to authorized subjects only and existing systems can be used for storage only. In summation, the Gemini computer can only serve as a guard device for a predetermined subset of the information that is created, stored, or processed in the facility.

2. The Gemini Computer as a Basis For Multilevel Security

Other than the research aspect, Gemini's greatest contribution would be the capability of providing a multilevel secure environment for all information handling functions in the W.A.R. lab. Unfortunately, without the prohibitive investment of several man-years, the existing systems and resident software cannot qualify for the stringent requirements demanded by the Gemini's TCB. Most of the reasons were mentioned in the previous section. Primarily, existing systems do not have a TCB and the complexity of resident software (esp. operating systems and wargames) make it extremely difficult for them to be adapted to the Gemini system.

In order to maintain a sphere with multilevel security, the Gemini base must be used for creating, storing, or processing all information that is to be dynamic within the environment. The Gemini system supports several processors and memory expansion to provide a complete multilevel secure system within itself. Also, memory can be partitioned on the existing system for exclusive use by the Gemini system. A major drawback is the fact that future software development must proceed around the requirements of the Gemini system. Until such a system is standardized in the military community, transportability of software will be limited.

The shortcomings listed are not only associated with the Gemini system, but rather apply to all "bolt-on" multilevel secure systems. They are not indicative of a lack of sophistication, but of the complexity of providing multilevel security.

VI. CONCLUSION

A. CONCLUDING REMARKS

The original intent of this paper was to examine the integration of the Gemini Trusted Multiple Microcomputer Base into the W.A.R. lab and to develop a framework for converting the facility into a multilevel secure environment. During the research phase of preparing this paper, it was discovered that the so-called "bolt-on" security systems currently available are extremely limited as a means for creating a multilevel secure environment if the goal is to use the processing capability and resident software of existing computing systems. Thus, the direction of this paper was changed to assess the security risk currently associated with the W.A.R. lab and to establish bounds for the integration of the Gemini system.

The need for a multilevel secure environment continues to be a limiting factor in the realization of the full potential of automated data processing systems used for sensitive information. Given the complexity of the security problem and the safeguards that are enforced by the Trusted Computing Base (TCB), it is unlikely that any retrofitted security system can be meshed with an existing computer system and its resident software to produce a complete multilevel secure environment. "Bottom-up" design, as seen in the Blacker project, appears to be the best alternative for very large information processing systems.

The integration of the Gemini Trusted Multiple Microcomputer Base into the W.A.R. lab will not convert the facility into a complete multilevel secure environment. However, the Gemini system is a formidable information processing system that can provide a multilevel secure environment by itself. Also, the Gemini system's capabilities can be greatly enhanced by the addition of multiple processors and information storage devices. Discounting the research opportunities, the Gemini system's greatest contribution to the W.A.R. lab will be its role as a secure guard for enforcing discretionary access.

B. RECOMMENDATIONS FOR FOLLOW-ON STUDY

The Gemini system will provide an excellent vehicle for graduate level research for both centralized and distributed secure information processing in the C3I environment. The Computer Science Department is currently conducting research on a Gemini system that was recently acquired; thus, a close liaison must be maintained with the Computer Science Department to prevent duplication of effort. A clear division of work should be established. The Command and Control curriculum should restrict research projects to those that are application (system level) or security policy oriented.

The following is a suggestive list of feasible areas of study:

1. Integration into existing untrusted systems - There are many untrusted information processing systems within the Department of Defense that could benefit from "guard" technology. The need to pass information between untrusted systems at different security levels is great and becoming increasingly more necessary at all levels within the armed forces. This ability could also eliminate some of the redundancy seen in existing systems. The development and demonstration of a trusted "guard" device between The Marine Corps Tactical Combat System (TCO) and the Marine Air Ground Intelligence System (MAGIS) is one example.

MAGIS is an integrated tactical data system which will provide the Marine commander with timely, accurate and complete all-source intelligence on which to base tactical decisions. TCO will be an on-line, interactive, secure tactical command and control system designed to enhance the capability of the commander and his operational staff to conduct combat operations and planning. TCO's role is below wing and division level where MAGIS is not resident. The need exists for a security device which provides a virtual link between end-user (TCO) to end-user (MAGIS) but can cause a physical break in order to allow message traffic between SCI and non-SCI systems. The TCO will serve as the primary source of information for MAGIS.

2. Reduction in throughput - Obviously, the additional processing required to enforce a well-formulated security policy reduces the total throughput of the system. The degree of security labelling can range from the byte level, to the word level, to the file level. The lower the level that labelling is required, the greater the cost in throughput time. Research is needed to establish how much degradation in throughput can be tolerated for individual applications and to examine the trade-offs.

3. Policies concerning data aggregation - It is possible for an aggregate set of data elements to be of a higher sensitivity level than those data elements taken individually. Areas where this situation is likely to be a problem need to be identified and safeguards developed.

Regardless of the area of study, the researcher must be aware of the considerations discussed during the risk assessment chapter and answer the question: "Is the level of effort (both time and money) required to achieve the desired security environment commensurate to the value of the protected information?"

APPENDIX A - SECURITY MODES OF OPERATION

DoD computer security policy identifies five modes of operation to accredit automated systems that process classified information:

Dedicated - All system equipment is used exclusively by that system and all user's have equal access (both level of classification and need-to-know) to the information on that system.

System High - All system equipment is protected at the level of the most sensitive information that is processed by that equipment. Users are cleared to that level, but may not meet need-to-know requirements for some of the information.

Multilevel - The environment is the same as the controlled - users without the proper level of clearance and/or need-to-know for all information that is processed on the system; however, in this mode, the operating system and associated system software are responsible for the separation of users and classified material.

Controlled - System users do not necessarily have the proper level of clearance and/or need-to-know for all information that is processed on the system. The burden of separation of users and classified information is not essentially under operating system control.

Compartmented - System allows two or more types of compartmented information or any one type of compartmented information with other than compartmented information to be processed. System access is secured to at least Top Secret, but all users need not be formally authorized access to all types of compartmented information being processed and/or stored in the system.

Additional policies may be defined to reflect the needs of the individual services.

APPENDIX B - SECURITY CLEARANCES

The following is a detailed description of security clearances as used by the DoD Computer Security Center:

a. Uncleared (U) - Personnel with no clearance or authorization. Permitted access to any information for which there are no specified controls, such as openly published information.

b. Unclassified Information (N) - Personnel who are authorized access to sensitive unclassified (e.g., For Official Use Only (FOUO)) information, either by an explicit official authorization or by an implicit derived from official assignments or responsibilities.

c. Confidential Clearance (C) - Requires U.S. citizenship and typically some limited records checking. In some cases, a National Agency Check (NAC) is required (e.g., for U.S. citizens employed by colleges or universities).

d. Secret Clearance (S) - Typically requires a NAC, which consists of searching the Federal Bureau of Investigation fingerprint and investigative files and the Defense Central Index of Investigations. In some cases, further investigation is required.

e. Top Secret Clearance based on a current Background Investigation (TS(BI)) - Requires and investigation that consists of a NAC, personal contacts, record searches, and written inquiries. A BI typically includes an investigation extending back 5 years, often with a spot check investigation extending back 15 years.

f. Top Secret Clearance based on a current Special Background Investigation (TS(SBI)) - Requires an investigation that, in addition to the investigation for a BI, includes additional checks on the subject's immediate family (if foreign born) and spouse and neighborhood investigations to verify each of the subject's former residences in the United States where he resided six months or more. An SBI typically includes an investigation extending back 15 years. [Ref. 10:p. 27]

The following two categories are actually authorizations rather than clearance levels, but they are included to emphasize their importance.

g. One category (1C) - In addition to a TS(SBI) clearance, written authorization for access to one category of information is required. Authorizations are the access rights granted to a user by a responsible individual (e.g., security officer).

h. Multiple categories (MC) - In addition to TS(SBI) clearance, written authorization for access to multiple categories of information is required. [Ref. 10:p. 28]

Data sensitivies or classifications can also be defined that are grouped using the same hierarchy as above, but are not limited to these categories. NOFORN is one such nonhierarchical sensitivity category.

APPENDIX C - PROJECTS TO DEVELOP TRUSTED SYSTEMS

Appendix C consists of three tables extracted from Carl E. Landwehr's "The Best Available Technology for Computer Security" which appeared in the July 1983 issue of Computer magazine.

Table C.1 - Completed Projects to Develop Trusted Systems

Table C.2 - Projects Underway to Develop Trusted Systems

Table C.3 - Abbreviations Used in Appendix C

TABLE C.1 - COMPLETED PROJECTS TO DEVELOP TRUSTED SYSTEMS

Project	Initiated	Sponsors	Builders	Goals	Approach	Formal Spec	Verification	Hardware	Prog Lang	Perf.	Cert	Est Eval	Installations
Adept-50	1967	DARPA	SDC	General-purpose time-sharing with security	High-water-mark model, labeled objects	No	No	IBM/360	asm MDL/360	Yes	System high	B-1	Pentagon, CIA, SDC
Multics Security Enhancements	Early 70's	AF, Honeywell	Honeywell, Mitre	General-purpose time-sharing with security	Retrofit checks for Bell-LaPadula model	No	No	Honeywell 6180 DPS8/70M	PL/I	Yes	Controlled	B-2	Pentagon AFDSC [DoD CSEC]
Mitre Brassboard Kernel	Early 70's	AF	Mitre	Prototype security kernel	Bell-LaPadula model as basis	Yes	Manual	PDP-11	SUE-11	Demo	No	A-1	Mitre
UCLA Data Secure Unix	Early 70's	DARPA	UCLA	Unix with security	Security kernel plus Unix emulator	Yes	Some	PDP-11	UCLA-Pascal	Demo	No	A-1	UCLA
Military Message Experiment	Late 70's	DARPA, Navy	ISI, BBN, MIT	Multilevel secure message system experiment	Simulated security kernel interface built on pseudokernel	No	No	PDP-10	Bliss BCPL,?	Yes	System high	B-2	Cincpac
Share-7	Mid-70's	Navy	FCDSSA	General-purpose timesharing with security	Based on virtual machine monitor architecture	No	No	AN/UYK-7	CMS-2	Yes	[Controlled]	B-1	FCDSSA sites
Secure Archival Storage System	1978	Navy	Naval PG School	Secure archival file system	Multi-microprocessor-based kernel	No	No	Zilog 8000	asm	Demo	[Multi-level]	B-3	Naval PG School
Damos	1979	Christian Rovsing	Christian Rovsing	Operating system for communications	Security kernel with trusted processes on capability architecture	Vienna Defn. Lang.	No	CR8D	?	Yes	System high	B-2	?
Autodin II	Late 70's	DCA	Western Union, CSC, FACC	Multilevel secure packet switch	Security kernel architecture	Yes Ina-Jo	Yes ITP	PDP-11	C asm	?	[Multi-level]	B-3	2 test sites
SDC Communications Kernel	Late 70's	DoD	SDC	Multilevel secure packet switch	Tailor UCLA Unix security kernel	No	No	PDP-11	UCLA-Pascal	Yes	[Multi-level]	B-2	SDC, DoD
Message Flow Modulator	1981	Navy	Univ. Texas	Filter message traffic	Trusted processes directly on hardware, code verification	Gypsy	Gypsy	LSI-11	Gypsy	Yes	[Multi-level?]	C-2	[OSIS]

TABLE C.2 - PROJECTS UNDERWAY TO DEVELOP TRUSTED SYSTEMS

Project	Initiated	Sponsors	Builders	Goals	Approach	Formal Spec	Verification	Hardware	Prog Lang	Perf	Cert.	Est Eval	Installations
KVM/370	1976	DARPA, AF, DCA	SDC	General-purpose time-sharing with security	Retrofit security kernel to virtual machine simulator	Yes Ina-Jo	Yes ITP	IBM 4331	Jovial J3	Demo	[Multi-level]	A-1	Mitre, SDC
PPSN (SUE)	1977	RSRE	RSRE	End-end encryption packet switch	Kernel implementing virtual machines	Some	Some Manual	PDP-11/34	asm Coral 66	Yes	?	C-2	RSRE
KSOS	Late 70's	NSA, DARPA, Navy	FACC, Logicon	Production prototype, secure UNIX	Security kernel with Unix emulator, trusted processes	Yes Special	Yes Boyer-Moore	PDP-11	Modula	No	[Multi-level]	A-1	Logicon, Mitre
Scomp	Late 70's	Honeywell, DARPA DCA, NSA Navy	Honeywell	Production prototype, secure UNIX	Security kernel with Unix emulator, trusted processes, hardware assistance	Yes Special	Yes Boyer-Moore	Honeywell Level 6	UCLA-Pascal C	NC	[Multi-level]	A-1	Mitre, DoD CSEC, Logicon
Sacdin	Late 70's	AF	ITT, IBM	Secure communications processor	Security-kernel-based architecture	Yes TLS Special	Yes TLS Boyer-Moore	IBM Series 1	asm	NC	[Multi-level]	A-1	[SAC sites]
Guard	Late 70's	Navy, DARPA	Logicon	Sanitize filter between DBMSs	Trusted processes on KSDS	Some Gypsy	Some Gypsy	PDP-11	C,Modula	NC	[Multi-level]	B-1	?
COS/NFE	Late 70's	DCA	Compion (DTI)	Multilevel secure network front end for WWMCCS	Security kernel (Hub), trusted modules	TLS SLS Ina-Jo	TLS SLS ITP	PDP-11	Pascal	NC	[Con-trolled]	A-1	[Demo only]
DEC DS Security Projects	1979	DEC	DEC	Add security to VMS, Tops-20	Retrofit Bell-LaPadula security checks (Tops-20, VMS), build kernel (VMS only)	[Yes Kernel only]	[Yes Kernel only]	DEC-20 VAX-11	?	NC	[Multi-level]	B-1-A-1	[DEC]
Forscom Guard	1980	DCA, WIS/JPM	Logicon, Honeywell	Filter traffic between host and terminals	Trusted processes on security kernel	Yes Gypsy	?	Scomp	C	NC	[Multi-level]	B-3	Forscom
LSI Guard	1980	Navy	I P Sharp	Guard system for single user	Trusted processes on bare hardware	Yes Euclid	[Yes]	DEC LSI-11	Euclid	Yes	[Multi-level]	B-3	[Navy]
PSDS	1980	NSA	FACC, Honeywell	Secure capability-based operating system	Formally specify and verify entire OS	Yes	Yes Manual	Honeywell (new)	Ada	NB	[Multi-level]	A-1	

TABLE C.2 - PROJECTS UNDERWAY TO DEVELOP TRUSTED SYSTEMS (CONTINUED)

Project	Initiated	Sponsors	Builders	Goals	Approach	Formal Spec	Verification	Hardware	Prog Lang.	Perf.	Cert	Est. Eval	Installations
RAP Guard	Early 80's	NASA	CSC, Sytek	Filter terminal-host communications no operator	Trusted processes on trusted task monitor	[TLS Special]	Yes Manual	Intel 286 VAX-11/730	?	NC	[Controlled]	A-1	[NASA]
SDC Secure Release Terminal	1981	SDC	SDC	Trusted release station (guard)	Trusted processes on bare hardware	TLS SLS 3LS Ina-Jo	TLS [SLS] ITP	LSI-11 [Intel 8086]	Modula	Yes	[Multi-level]	A-1	SDC, (DoD)
Recon Guard	1981		Sytek	Guard between network and database	Trusted processes, encryption-based authentication	No	No	Intel 8086	Pascal	NC	[Multi-level]	B-3	
GSDS	1982	Gemini Corp	Gemini Corp	Secure real-time operating system	Security kernel architecture	[TLS SLS]	No	Intel 286	PLM PL/I	NC	[Multi-level?]	B-3	?
Distributed Secure System	1982	RSRE	SDL Ltd, MARI	General-purpose multilevel secure local net	Trusted network interface	[Yes Euclid]	[Yes]	PDP-11	[Euclid]	NC	[Multi-level]	A-1	[RSRE]

TABLE C.3 - ABBREVIATIONS USED IN APPENDIX C

Notes:

? data unknown or uncertain
[] enclosed data indicates plans, not accomplishments

Abbreviations:

AF	Air Force
AFDSC	Air Force Data Services Center
asm	Assembly language (for machine indicated)
BBN	Bolt Beranek and Newman, Inc.
Boyer-Moore	Boyer-Moore theorem prover (SRI)
CIA	Central Intelligence Agency
Cincpac	Commander-in-Chief, Pacific
CSC	Computer Sciences Corp.
DARPA	Defense Advanced Research Projects Agency
DEC	Digital Equipment Corp.
Demo	System built as prototype or demonstrator only
DCA	Defense Communications Agency
FACC	Ford Aerospace and Comm. Corp.
FCDSSA	Fleet Combat Direction Systems Support Activity
Forscom	Forces Command (Army)
ISI	Information Sciences Institute
ITP	Interactive theorem prover (SDC)
MARI	Microprocessor Applications Research Institute (England)
MOL/360	Machine Oriented Language for IBM/360
NASA	National Aeronautics and Space Administration
NB	System never built
NC	System not yet complete enough for evaluation
NSA	National Security Agency
RSRE	Royal Signals and Radar Establishment (Malvern, England)
SDC	System Development Corporation
SDL	System Designers, Ltd. (England)
SLS	Second-level specification
SRI	SRI International
TLS	Top-level specification
VMS	Operating system for DEC VAX computer
WIS/JPM	WWMCCS joint program manager
WSE	WWMCCS system engineer
WWMCCS	World-Wide Military Command and Control System
3LS	Third-level specification

APPENDIX D - W.A.R. LAB COMPUTING RESOURCES

A. PROCESSING HARDWARE

(1) VAX - 11/780 with:

6 MB Main Memory

1200 MB Virtual Disk Memory

High Speed Printer

16 Terminals

(3) RAMTEK Hi-Res Graphics Systems with:

Dual Monitors

Tablets

(3) WICAT/NAVTAG Microprocessor-based Tactical Trainers

B. COMMUNICATION HARDWARE

(1) Private Line Interface (PLI)

(1) Crypto Generator (KG-34)

(1) ARPANET IMP (C-30)

C. SOFTWARE/FIRMWARE

VAX VMS Operating System with:

Fortran 77 Compiler (For NWISS/IBGTT Development)

Simscript Compiler (For JTLS Development)

Berkeley UNIX (4.1 BSD) with:

C Compiler

Pascal Compiler

Lisp Environment

Graphics Tools Package (DI-3000)

Statistical Tools Package (SPSS-X)

D. SIMULATIONS/MODELS

NWISS (IBGTT)

JTLS

COMEL

WAAM (Incomplete)

JANUS (Replay Files Only)

E. MICROSYSTEMS

Fleet Mission Program Library

Decision Aids Implemented On:

HP 9020 (Standard)

Others (Wang, Tandy)

NAVTAG

Surface Warfare Trainer

Microcomputer Graphics

Videodisc Map Overlay

APPENDIX E - GEMINI TRUSTED MULTIPLE MICROCOMPUTER BASE - PRODUCT DESCRIPTION

CAPABILITIES:

- **Concurrent computing.** Gemini operating system supports up to 8 powerful iAPX286 processors for combined parallel and pipeline concurrent processing.

- **Flexible multilevel security.** Designed as DoD Class B3 multiprocessing security kernel, coded in Pascal, with hardware-supported DES encryption.

- **Configuration independence.** Supports various configurations from a real-time dedicated controller to a multi-user workstation.

- **Self-hosted software development.** Disk-based CP/M environment and Gemini tools for applications in Pascal, JANUS ADA, C, PL/I and FORTRAN.

ARCHITECTURE:

- IEEE Standard 796 Multibus.

- Microcomputers based on the Intel iAPX286 microprocessor with CPU and MMU on one chip.

- Up to 8 microcomputers tightly coupled on bus.

- Up to 2 Mbytes local RAM per microcomputer.

- Up to 8 Mbytes shared global memory per system.

- Up to 4 disk drives with any mix of fixed Winchester, removable Winchester and floppy diskettes.

- Up to 24 RS-232 serial I/O interface ports.

- Real-time calendar clock with battery backup.

- High speed DES data encryption hardware.

- Non-volatile system password and encryption key storage.

SYSTEM SOFTWARE:

- Gemini Multiprocessing Secure Operating System (GEMSOS). Compatible in all configurations.
- Separation and sharing of data based on sensitivity and integrity levels and compartments.
- DoD Computer Security Center Development Product Evaluation in progress.
- Convenient interface to GEMSOS for concurrent computing application programs in several programming languages.
- Gemini development tools for concurrent computing applications.
- Same GEMSOS on every processor. Completely distributed operating system.

LIST OF REFERENCES

1. Klein, Melville H., "Computer Security", Issues in C3I Program Management, Ed. Jon L. Boyes, AFCEA International Press, 1984.

2. Pritchard, J. A., Computer Security: Risk Management in Action, NCC Publications, 1978.

3. Landwehr, Carl E., "The Best Available Technology for Computer Security", Computer, Vol. 16, No. 7, July 1983.

4. Ames, Jr., Stanley R., Gasser, Morrie, and Schell, Roger R., "Security Kernel Design and Implementation: An Introduction", Computer, Vol. 16, No. 7, July 1983.

5. Scharf, James D., Wallentine, Virgil, and Fisher, Paul S., "DoD Network Security Considerations", Advances in Computer Security Management - Volume 1, Ed. Thomas A. Rullo, Heyden & Son, Inc., 1980.

6. DoD Computer Security Center, Department of Defense Trusted Computer System Evaluation Criteria, CSC-STD-001-83, 15 August 1983.

7. DoD Computer Security Center, Department of Defense Trusted Network Evaluation Criteria, (Draft) 29 July 1985.

8. Nelms, Kenneth L., Security/Privacy Considerations in Data Processing, Master's Thesis, Naval Postgraduate School, Monterey, California, March 1979.

9. Helling, William D., Computer Security for the Computer Systems Manager, Master's Thesis, Naval Postgraduate School, Monterey, California, December 1982.

10. DoD Computer Security Center, Technical Rationale Behind CSC-STD-003: Computer Security Requirements -- Guidance for Applying the Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments, CSC-STD-004-85, 25 June 1985.

11. Naval Research Laboratory Report 8897, An Approach to Determining Computer Security Requirements for Navy Systems, by Carl E. Landwehr and H. O. Lubbes, 13 May 1985.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, Virginia 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, California 93943-5002	2
3.	Major Thomas J. Brown, Code 62 Bb Command, Control, and Communications Academic Group Naval Postgraduate School Monterey, California 93943-5000	2
4.	Professor Michael G. Sovereign, Code 74 Chairman Command, Control, and Communications Academic Group Naval Postgraduated School Monterey, California 93943-5000	2
5.	CPT James A. Wall P.O. Box 644 Ft. Knox, Kentucky 40121	1